2023 年国内 APT 攻击威胁年报

电信安全水滴实验室

2024 年 2 月

地址：北京市东城区朝阳门北大街 19 号 4 层[1]
网址：www.ctct.cn
电话：400-925-9120

目录

天下大势，攻久必知，知久必防，没有网络安全就没有国家安全。传承红色电信精神，作为中国电信建设安全型企业的主力军，电信安全承担中国电信网络安全关键核心技术创新的主体责任，是国家关基安全的重要科研力量。电信安全将持续贯彻落实数字中国发展战略要求，为网络强国和数字中国建设贡献电信力量！

1. 概述

电信安全水滴实验室在狩猎 APT 攻击威胁中发现，2023 年国内被 APT 攻击态势呈饱和式攻击状态。APT 威胁狩猎系统建设运营半年来，追踪 10 多个常年活跃于国内的 APT 组织，发现 APT 事件 871 起，多个专项行动，确定攻击对象单位 300+，覆盖航空航天、JG、GF、能源、金融、科研、教育、医疗、外交、外贸、边防、大基建、数字化供应链等十多个行业。不同的 APT 组织由于地缘和时政的差异与变化，攻击的侧重需求、行业和对象都存在差异。

图-（2024/3/12）APT 威胁狩猎全局概览

2023 年国内 APT 事件 Top5 省/自治区/直辖市/生产兵团/特区（统称：省）依次是北

京、广东、江苏、浙江、上海。从攻击频率评估，当前国内面临 APT 攻击的威胁依次是来自东南亚、南亚、台海、东北亚、东欧、欧美等地区；从攻击武器库复杂度、发现难度和造成影响等维度评估，则依次是来自欧美、东欧、东北亚、台海、东南亚、南亚。

结合 2023 年 APT 攻击态势预测 2024 年的 APT 攻击威胁，从行业侧预测重点是数字化政务、JG、GF、高新科技（通信：5G、卫星通信、量子通信、骨干路由、大型计算，芯片：设计、制造、GPU，自动化：大型制造：船舶、高铁、机器人，新能源：能源存储）、能源系统、金融系统、教育系统、交通系统等；从攻击手法预测是本土化安全设备或云办公系统通用漏洞批量化攻击，上游供应链攻击，非传统模式攻击，APT 与勒索双模式结合攻击。

电信安全水滴实验室预计，相较往年，2024 年的 APT 攻击威胁将呈现更为严峻的情况。如何做好 APT 攻击威胁控制？则需要从多维度、多层次做综合评估和联合举措。电信安全水滴实验室认为做好 APT 攻击威胁管控，需要从宏观角度落地以下举措：

- 建设国家体系化的前置狩猎假想威胁，从攻击幕后背景需求假想攻击行业、对象、方式，主动对假想行业的重点企业进行风险狩猎；
- 建设体系化的主动威胁狩猎，全面常态化前置攻击风险监测，打通威胁从狩猎、监测、分析、预警、响应、阻断、排查、溯源、链路还原、画像、反制、加固、复盘、全网评估的闭环；
- 国家监管统筹全局，安全厂商风险狩猎，全面风险评估，企业落地响应的多方协同，形成将攻击事件点快速转化同源攻击专项行动的效果，实现全面化的主动防御和前置预警的联防联控效果；

2. 2023 年 APT 攻击威胁态势详情

真正具备 APT 能力的攻击，其本质目的大概有：

- 长期潜伏攻击对象内部网络，采集内部高价值数据作为有效情报信息，为幕后背景国家智库做政策提供依据，为幕后国家外交政治谈判提供筹码，为幕后国家军事、科技等发展提供科研成果；

- 控制攻击对象核心生产设备必要时期制造极限安全场景，引起社会恐慌，影响 ZF、社会、经济、军事、民生混乱，利用舆情左右敌对国家的发展甚至决定战争结局的走向；

当然，不同的 APT 组织由于地缘和时政的差异与变化，攻击的侧重、需求、行业和对象均存在差异。例如，东南亚方向的 APT 组织偏向于海洋、能源、政务、JG、GF、科研、教育和数字化等；南亚方向的 APT 组织偏向于军贸、航空航天、外交和高校等；东北亚方向的 APT 组织偏向 JG、GF、人工智能和机器人等行业；台海方向的 APT 组织偏向于台海军情、JG、GF、高校、科研等；欧美方向的 APT 组织偏向于 JG、GF、ZF、外交和先进科技等；东欧方向的 APT 组织偏向运营商、数据中心、能源等。

2.1.东南亚方向

攻击国内资产最为频繁的区域 APT 组织当属东南亚方向，可以说是“马克沁机枪”式攻击。在 2023 年，发现该区域 APT 组织多次利用在野 0/Nday 漏洞对国内资产展开专项行动攻击，其中包括“尼格风暴”、“暗云风暴”、“丝绸风暴”[1]等专项行动，仅专项行动就造成攻击事件约 300 个，占全部攻击事件的 36%。

在攻击手法上，除了常态化定向钓鱼攻击投递木马外，还比较倾向于收集 HW 或本土在野 0day 漏洞的武器库化利用，以期达到批量攻击效果，不过攻击的对象行业略显模糊。当然，批量攻击只是对攻击对象的泛化“抓鸡”，后期还会对攻击对象筛选，如果发现其中有敏感的高价值对象则会进行深入内网横移窃取敏感信息，扩大攻击成果。此外，根据目前掌握的攻击案例线索了解，针对难以正面突破的行业对象（例如能源、金融等），攻击者一直尝试从上游供应链侧攻击，例如能源智能化管理设备供应商，办公软件供应商，安全设备供应商等。

整体而言，东南亚 APT 组织攻击覆盖的行业比较广泛，因为攻击对象是从空间测绘中批量采集互联网暴露的服务资产，所以该组织的攻击对象行业覆盖海洋、能源、政务、JG、GF、科研、教育、数字化、外贸、互联网、医疗、能源、边防等十多个行业。

2.2.南亚方向

南亚方向 APT 最为繁盛，大小组织汇总似有十多个，比较常见活跃于国内的有 Patch

[1] “尼格风暴”、“暗云风暴”、“丝绸风暴”：电信安全发现并命名的专项攻击行动。

work（白象）、Sidewinder（响尾蛇）、Bitter（蔓灵花）、CNC 等，他们的攻击方式和攻击对象也存在较多共性。攻击方式以钓鱼邮件为主略显简单粗暴，整体武器库的迭代周期较长，攻击行业则偏向于高校科研、对外军贸、航空航天、外交、ZF 等。

看似平平无奇的 APT 组织群，但广撒网模式的高信誉钓鱼，也是蛮狠的，且每个组织都有自己的特点，例如：Patchwork 倾向于高校科研和外交，Sidewinder 倾向攻击对外军贸和高校科研，Bitter 倾向于攻击高校科研和外贸，CNC 倾向于攻击高校科研和航空航天。因此，在各组织间似乎除了分工配合之外，还略带少许“内卷”，不过整体的方向还是一致的，既收集重要的外交信息，获取中国向巴基斯坦、中东、南亚地区的对外军事贸易，窃取航空航天方向的重大科研成果。

在南亚地区的诸多 APT 组织中，比较突出的当属 CNC，该组织长期针对国内航空航天行业攻击，并在 2023 年 1 月至 7 月间针对国内多个航空航天单位展开专项攻击，且疑似存在窃取科研数据迹象，我们将本次专项命名为“九霄行动”。

2.3. 东北亚方向

由于东北亚局势的长期不稳定因素，造成各方 APT 组织势力处于长期活跃状态，例如 Lazaruz（拉撒路斯）、Kimsuky、ClickOnce（旺刺）和 Darkhotel（黑店）等组织。如今的 Lazaruz 和 Kimsuky 似乎背上了“不该有”的业绩创收压力，业务纷纷转向了盗取虚拟加密货币变现外汇，不过 ClickOnce 和 Darkhotel 依然活跃于 APT 战线上，但攻击方向并非朝鲜半岛，而是转向了中国。ClickOnce 和 Darkhotel 其幕后背景都隶属于某军情部门，在 2023 年底均发现其在国内的攻击痕迹。

ClickOnce 组织在 2023 年 10 月至 12 月对国内资产展开攻击，攻击对象涉及智能电网配控企业、疑似涉军相关人员和多个国内知名大学科研人员。

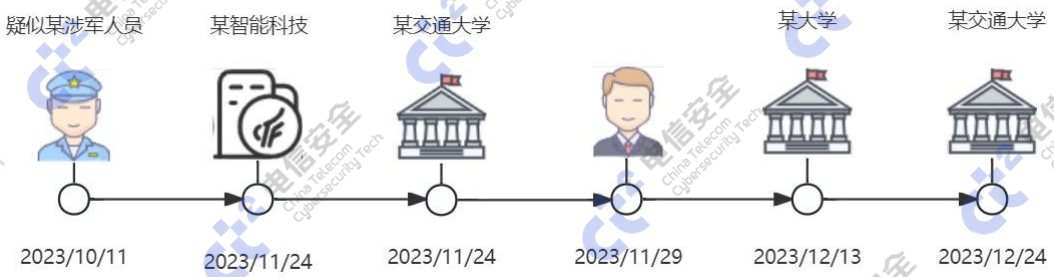


图-ClickOnce 组织攻击国内资产复现

同样，在 2023 年 10 月至 2024 年 1 月，Darkhotel 组织对国内展开密集钓鱼攻击，攻击对象涉及 30 多个，且主要以 JG 单位为主，其目的是窃取终端敏感数据加密回传境外。因此，我们将本次专项行动命名为“军刀行动”。

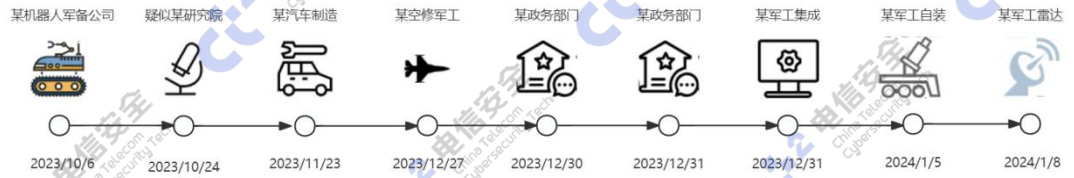


图-Darkhotel 组织攻击国内资产复现

2.4.台海方向

台海方向的 APT 组织目前比较活跃的是 Greenspot（绿斑），其仍持续对境内高校、智库、ZF、外贸、海事、JG、GF 等行业做常态化钓鱼攻击。“绿斑”的钓鱼攻击一般分为两个阶段，常见的网盘附件、邮箱登录下载模式，是广撒网的钓鱼攻击，主要是想采集攻击对象的个人邮箱账号和密码信息，之后，确定攻击对象，做高仿真攻击对象的邮箱登录系统诱导采集攻击对象员工邮箱账号信息，用于后期做高信誉钓鱼攻击。

可能地缘政治问题，该地区的 APT 组织也长期关注我国东南沿海的军情动态和边防警情。因此，常态化监视东南沿海军情、警情等机密信息可能是“绿斑”后期的需求方向，或许目前已经开始延伸，毕竟人为监视成本和风险都比较大。

2.5.欧美方向

2023 年 6 月和 12 月，知名安全厂商（卡巴斯基）先后两次披露疑似美国国家安全局（NSA）针对多国外交人员的“三角测量”专项攻击，利用多个 0day 组合，攻击者对外交人员的 iPhone 手机终端植入木马，以获取设备的 GPS、图片、通信记录、摄像头、通话录

音等敏感信息。

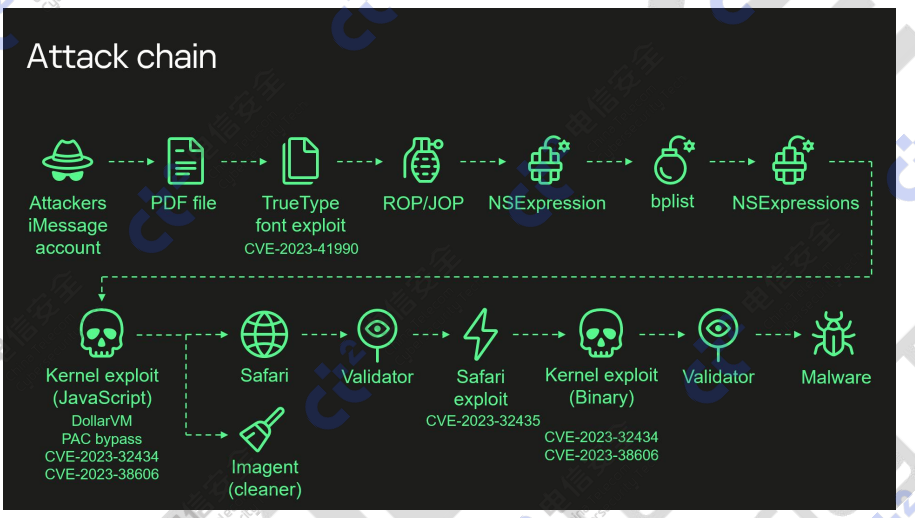


图-“三角测量”攻击链路（源卡巴斯基原图）

在 2023 年 7 月，国家计算机病毒应急处理中心和 360 公司监测发现，武汉市地震监测中心部分地震速报数据前端台站采集点网络设备遭受疑似欧美方向 APT 组织的网络攻击。如是属实，这或许可以揭开境外国家企图长期窥探并绘制针对我国的三维空间（军事、能源、交通）作战地图的真相。

图-拟真三维空间

对于后续欧美地区 APT 组织攻击对中国的攻击方向，初步预测大概在以下几个方向会面临比较大的风险：

- 延续“三维空间”作战地图行业（能源、交通）对象做高潜藏攻击，窃取最新最全最细空间信息；
- 持续对高敏感政务、外交、高新科研等行业做高潜藏攻击，窃取最新内部政务信息、

外交政策和重大科研成果；

- 向经济和金融等部门做高潜藏攻击，获取最新经济发展和金融发展规划；

2.6.东欧方向

在东欧地区，不仅滋养大批从事勒索、信息窃取、DDoS 攻击的黑产，也出现了不少的 APT 组织，例如 APT28、APT29、Sandworm、Gamdaredon 还有近期比较高调的 Blackjack 等组织。由于俄乌冲突的持续，双方网络空间作战已经进入白热化阶段，似有相互攻击运营商核心骨干网络，造成大面积网络中断，制造社会舆情恐慌，扰乱军心民意的迹象。这也说明网络战争深化不仅是基础的窃取情报数据，还有可能是瘫痪敌方核心关键基础设施，甚至起到连锁瘫痪敌方 ZF、医疗等机构的运行，配合热战实现最大化的对敌打击效果。在高度现代化、信息化、智能化时代，网络信息通信、高算力资产、能源产送网、交通运输网等，或将是极限场景下的重点攻击对象。

2.6.1. 乌克兰运营商 Kyivstar 遭到攻击

2023 年 12 月，乌克兰安全局宣称俄罗斯黑客攻破了乌克兰最大的电信服务提供商 Kyivstar 的系统，并清除了电信运营商核心网络上的所有系统数据。此次事件发生后，Kyivstar 的移动和数据服务中断，导致其 2500 万移动和家庭互联网用户中的大多数失去了互联网连接。

事件发生在持续化的俄乌冲突期间，黑客攻击运营商骨干网的承载系统，导致承载系统瘫痪，给乌克兰民生、经济、ZF 和军事等带来巨大的影响，是利用信息化战争辅助热战效果的典型案例。

2.6.2. 俄罗斯境内核心企业遭到报复式攻击

2024 年 1 月 16 日 黑客组织“Blackjack”声称，成功攻击了俄罗斯 IPL Consulting[2]，数十台服务器和数据库遭到破坏，摧毁了整个 IT 基础设施，导致超过 60 TB 的数据被删除，以回应此前乌克兰电信公司 Kyivstar 被攻击。

据悉，“Blackjack”还渗透到俄罗斯特殊项目主要军事建设局，下载了 1.2TB 数据，其中包括 500 多个军事站点的技术文档。该组织还向乌克兰武装部队传输了有关俄罗斯设施的关键情报。

[2] IPL Consulting：是一家在俄罗斯行业实施信息系统的公司，是俄罗斯最先进的企业之一，为汽车、航空、重型工程和 GF 领域的机构提供信息系统实施服务。

3.针对国内专项攻击详情

电信安全水滴实验室发现，在 2023 年期间，针对国内资产的专项攻击总计 8 起，其中包含 6 起境外 APT 攻击和 2 起勒索攻击。APT 攻击专项分别来自东南亚地区的"尼格风暴"、"暗云风暴"、"丝绸风暴"，南亚地区的"九霄行动"，以及针对能源行业的 APT&勒索双类型结合的专项攻击。勒索专项攻击分别为 Mallox 勒索团伙针对数据中心、芯片、生物制药、金融等行业的专项攻击和 BlackCat 勒索团伙针对高新制造、高质量发展类型企业的专项攻击。

3.1."尼格风暴"专项

2022 年 11 月 16 日 15:12 至 2023 年 4 月，追踪狩猎发现境外黑客利用国内某防火墙漏洞针对我国 ZF、JG、GF、医疗、能源、化工、地质等重点行业的 40 多个高价值企业资产展开攻击，存在较大的数据泄露风险。

图-威胁风险指数分析

攻击资产威胁风险显示，在 2022 年 12 月 17 日前后，本次专项行动的新型木马资产的威胁风险指数开始呈爆发性增长，攻击国内目标开始进入高发期，既"风暴中心"时期；2023 年 1 月中下旬威胁风险指数开始进入高位震荡，且风险指数峰值时间节点在 2023 年

1 月 31 日，对国内的短期战术攻击对象已经完成，暂停攻击新的目标；2023 年 2 月初，威胁指数显著下降，国内被攻击的目标已经进入威胁应急响应状态，攻击风险得到有效遏制和清除；2023 年 2 月至 4 月进入第二攻击阶段，并陆续攻击国内十多个资产。

从数据风险看，数据风险指数与威胁指数趋势基本吻合，但数据风险指数峰值的时间节点在 2022 年 12 月 31 日，可能对个别攻击对象进行高强度数据（通讯）交互（远程控制、数据传输、内网横移等）的场景，有较高的数据泄露风险。

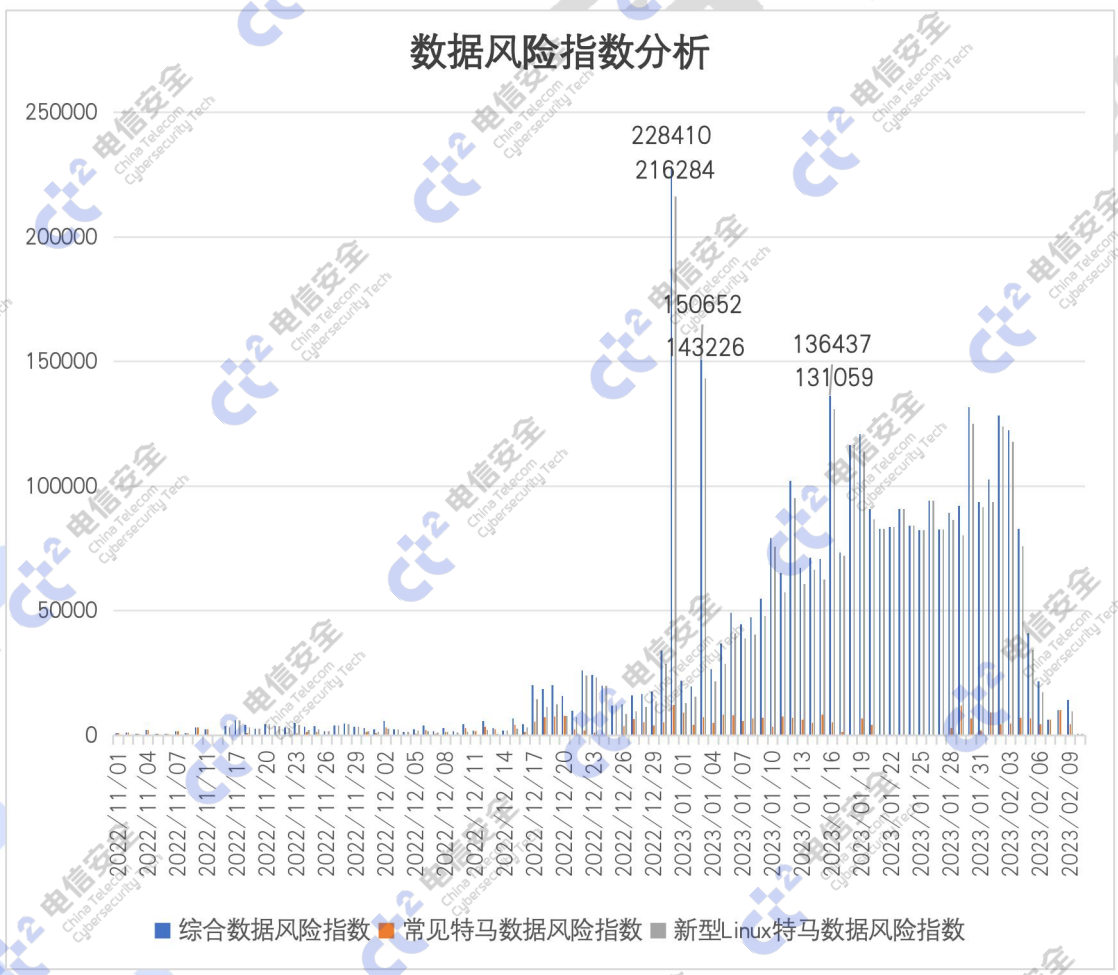


图-数据风险指数分析

由于本次 APT 攻击专项涉及目标范围大，且开始于 2022 年 11 月，与 2022 年的〝尼格〞热带风暴登陆我国大陆时间相近。因此，本次攻击专项代号命名为〝尼格风暴〞。

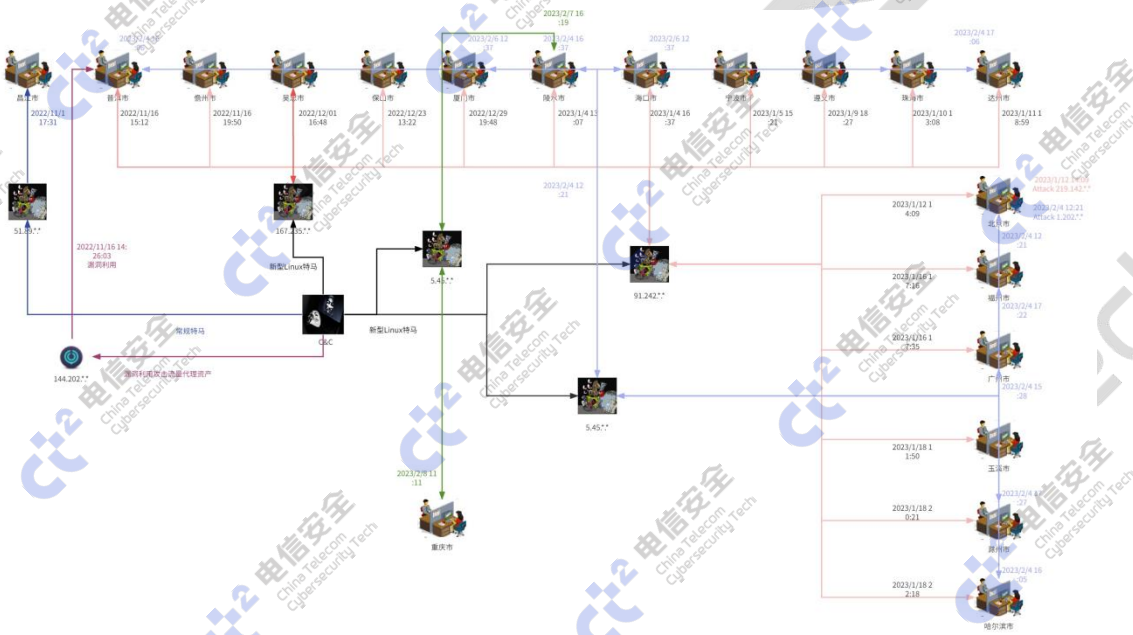


图-“尼格风暴”行动互联网攻击链路复盘

对“尼格风暴”攻击专项进行互联网攻击链路复原分析，主要复现其利用多个攻击节点对国内数十个攻击对象的攻击路线和模糊原始攻击时间点（同颜色代表同一攻击源），形成整个行动在互联网侧的大体攻击链路。关联复现攻击资产的攻击链路状态以及对国内各个攻击对象的初始攻击时间节点共性和交叉攻击等信息。对关联国内攻击对象做初步行业划分，疑似有涉及 ZF、JG、GF、医疗、能源、化工、地质、大基建等敏感行业。

3.2."九霄行动"专项

在 2023 年 1 月至 4 月，有境外 APT 组织伪造成国家科技部门做科研结果登记和项目申报通知等形式进行钓鱼攻击，邮件附件中嵌入后门恶意代码。

各相关研究室：

您好！为促进科技成果传播交流、为科技决策提供支撑，且部分奖励报奖前需提供成果登记证书，现院里组织开展科技成果登记工作（附件1）。

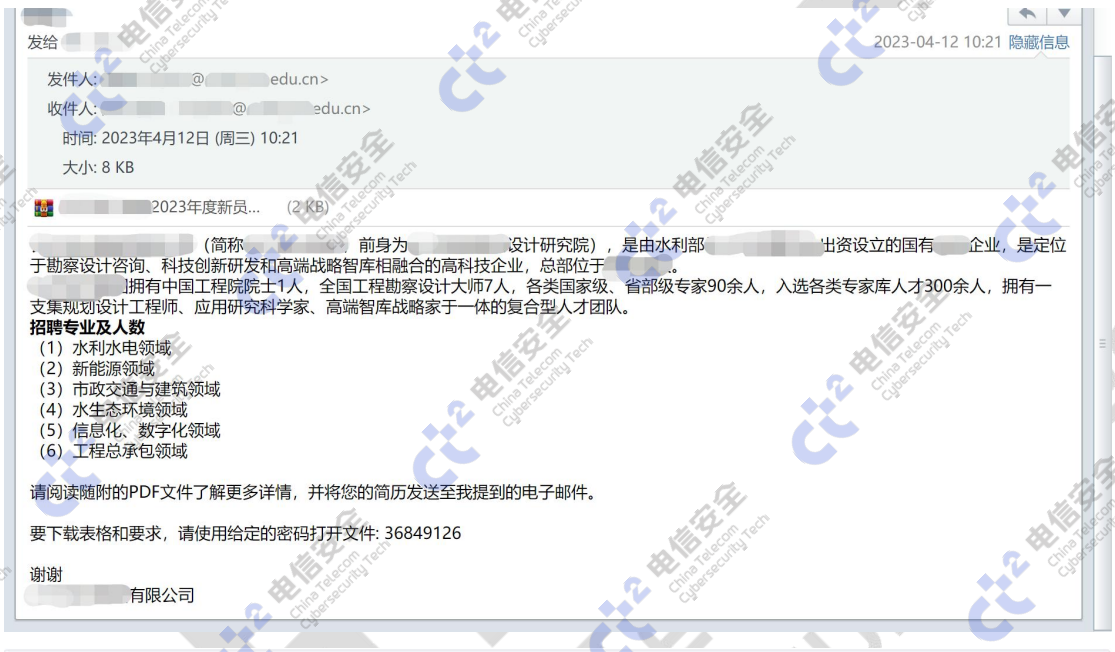
我们整理出今年已结题的项目（附件2），请各研究室秘书根据附件2中的本室项目，组织相关项目人员填报系统（填报方式见附件4，系统安装包见附件5），并填写登记表（附件3）。

最后将填报完系统后生成的压缩包以及附件3，在1月20日前，由各研究室秘书统一以研究室为单位反馈至本邮箱。

上报要求：1.使用本次发送的最新版“国家科技成果登记系统V11.0版”按要求填写后从系统中生成（.zip）压缩包文件；

2.按成果类型，选择附件3中的一项，录入成果名称，要与系统录入时选择的成果类型保持一致。

地址：北京市东城区朝阳门北大街 19 号 4 层
网址：www.ctct.cn
电话：400-925-9120



发给 [redacted] 2023-04-12 10:21 隐藏信息

发件人: [redacted]@[redacted]edu.cn>

收件人: [redacted]@[redacted]edu.cn>

时间: 2023年4月12日 (周三) 10:21

大小: 8 KB

[redacted]2023年度新员... (2 KB)

[redacted]（简称[redacted]前身为[redacted]设计研究院），是由水利部[redacted]出资设立的国有[redacted]企业，是定位于勘察设计咨询、科技创新研发和高端战略智库相融合的高科技企业，总部位于[redacted]。[redacted]拥有中国工程院院士1人，全国工程勘察设计大师7人，各类国家级、省部级专家90余人，入选各类专家库人才300余人，拥有一支集规划设计工程师、应用研究科学家、高端智库战略家于一体的复合型人才团队。

招聘专业及人数

（1）水利水电领域
（2）新能源领域
（3）市政交通与建筑领域
（4）水生态环境领域
（5）信息化、数字化领域
（6）工程总承包领域

请阅读随附的PDF文件了解更多详情，并将您的简历发送至我提到的电子邮件。

要下载表格和要求，请使用给定的密码打开文件: 36849126

谢谢

[redacted]有限公司

文件名称	类型	扫描时间	SHA256	多引擎检出	木马家族和类型	威胁等级
123.exe	EXEx86	2023-04-21 14:20:45	1a22dd2f6968e76c8c044d423cd592eb1bed01d2be6fc6df901437b593384ec9	8/22	Leonem 木马	可疑
先进结构与复合材料"等4个重点专项2023年度项目申报指南的通知 .pdf.lnk	Windows Shortcut(LNK)	2023-04-12 15:09:11	5c89e1bafa787294856acc458fd9021ddefa67d9826bc2234252db773a8212b5	4/22	Powedon 木马	恶意

图-钓鱼邮件样本

分析钓鱼邮件附件木马功能了解，木马利用白+黑模式+服务+计划任务+自启动实现长期潜伏失陷终端，利用组建配套模式实现终端敏感信息采集和加密传输。

数据窃取样本梳理分析					
文件名	执行机制	C2	样本落地时间	hash	功能
国家科技成果登记系统[V11.0].exe	即时模式加载释放木马	/	/	fa646df65d3a7b8eb5045b2ca7173b63	初始传播核心载荷
UpdateHelper.exe	/	/	/	f4ad7ba7e9ea0bb9d0704b1a56d3d041	白文件
国家科技成果登记系统用户操作说明v11.0.doc	/	/	/	7da4fe89100750eb6d70669e295eb427	诱饵文件（白）
YoudaoDictsrv.exe	注册服务：YoudaoDeskService	/	2023/01/11 20:21	3019b11ffb4f01d850f8ad93188ff5f	实现持久化
ZotUpdater.exe	/	/	2023/01/12 12:22	390f9430d01e499719e9a36af5489808	恶意功能组件
Tslwmc.exe	每天12:00（计划任务）	194.36.*.*:443	2023/01/12 12:25	04578f0c939858018accef45969e7f2e	窃密组件
known_hosts	/	文件内包含：194.36.*.*:49032	2023/01/12 12:36	/	后门组件
SumatraPDFUpdate.exe	每天15:00（计划任务）	2.58.*.*:49032	2023/01/17 20:28	5658b3a6cf75308ef3dc3842ef7ed50f	窃密组件
imagedrvhost.exe	自启动	146.59.*.*:443（情报关联）	2023/03/16 15:47	ce3b254fc75fe4210aa509581ca42848	恶意功能组件
sess.exe	/	/	2023/03/16 12:56	6ec600acf89ea212a8fcc8c96af7b566	浏览器窃密组件
sess_ch.bat	日志中发现执行记录，未找到实体文件	/		/	
coo.exe	日志中发现执行记录，未找到实体文件	/		/	

表-木马组件功能分析

从时间维度的攻击链路划分，本次攻击专项可划分 3 轮攻击。

地址：北京市东城区朝阳门北大街 19 号 4 层
网址：www.ctct.cn
电话：400-925-9120

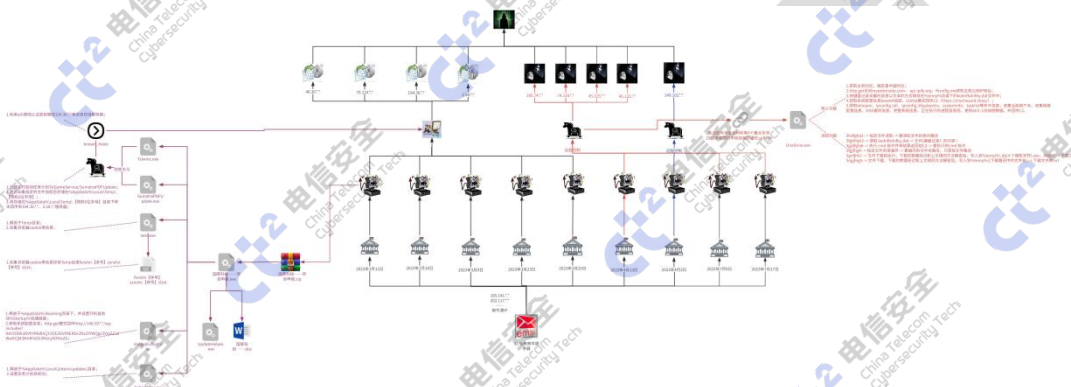


图-“九霄行动”攻击链路

从威胁风险指数上评估，第 1 轮攻击存在较为明显的差异，约是平均威胁风险指数的 6 倍，涉及 2 个攻击对象，且存在高达 90%的数据泄漏类型威胁风险比例，可能造成 36.49G 的数据泄露，属于本次攻击专项的重点攻击周期；第 2 轮攻击，涉及 2 个对象，可能造成 3.89G 的数据泄露，威胁风险指数略小于第 1 轮攻击；第 3 轮攻击，涉及 3 个对象，本轮攻击威胁风险峰值虽然略小于第 1 轮，可能造成 11.60G 的数据泄露，但是持续周期较长。

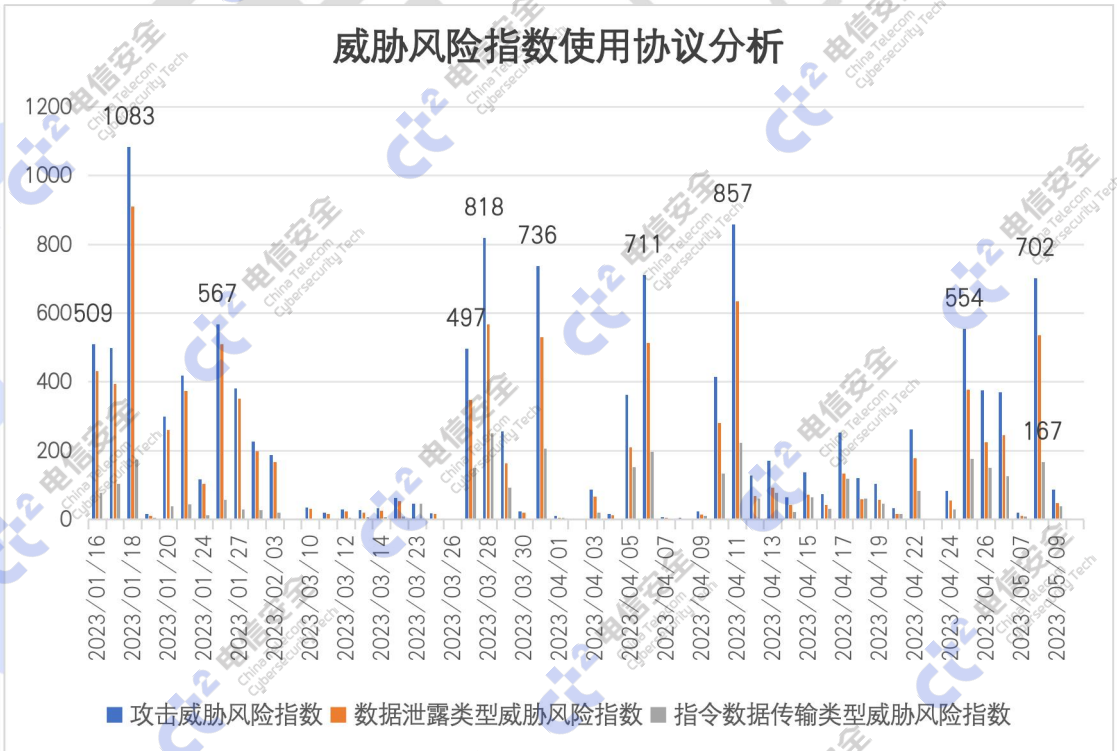


图-威胁风险指数分析

数据泄漏风险按照使用服务/协议分类分析，在 3 月前的早期攻击国内对象时主要使用 ssh，或许是为加强数据传输过程中的安全性，中后期的攻击仅一个攻击对象使用常规 tcp 协议传输外，其他攻击对象主要使用 https 安全加密协议传输。利用逆向估算数据泄漏分析模型计算，目前检测到国内的攻击对象可能造成 51.98G 的数据泄漏量，结合攻击对象行业

地址：北京市东城区朝阳门北大街 19 号 4 层
网址：www.ctct.cn
电话：400-925-9120

性质和总体数据泄漏风险指数评估，本次攻击专项危害性极大。

图-攻击数据风险指数分析

从攻击威胁日志中，筛选定位出 4 个攻击对象做详细风险数据指标分析。

关键指标 / 攻击对象	某 H 对象	某 B 对象	某 S 对象	某 Y 对象
风险系数星值	★★★★★	★★★★★	★★★★★	★★★★
高价值威胁风险权值	3347	2999	212	924
高价值数据风险权值	4362166	2620478	245585	73611
高价值数据泄漏风险权值	4322312	2492160	243129	41193
高价值指令数据传输风险权值	39854	128318	2456	32418
高价值威胁风险系数	418.375	66.64	26.5	115.5
高价值数据风险系数	2088.6	1618.79	495.6	271.3
高价值数据泄漏风险系数	2079.0	1578.65	493.1	203.0
攻击活动周期（天）	8	45	8	14
威胁等级系数	5	5	5	5
高价值综合风险系数（预警值>100）	23009.875	16545.4	5116.00	3019.00

地址：北京市东城区朝阳门北大街 19 号 4 层
网址：www.ctct.cn
电话：400-925-9120

数据泄漏风险占比	99.1%	95.78%	99.0%	56.0%
交叉感染木马量	2	2	2	3

表-攻击对象关键数据指标项梳理

在攻击者使用的手法、木马、攻击对象涉及的地域、行业等多个维度获取攻击画像指纹信息如下：

1.攻击使用的.lnk 嵌入后门代码，且与南亚地区背景的某 APT 组织攻击国内对象的常用手法吻合；

2.攻击使用的远程控制木马属于多组件功能组合模式，避免终端行为管理软件和杀毒软件拦截查杀。使用的攻击源资产远控服务端口指纹、远控木马代码片段指纹与南亚地区背景的某 APT 组织历史攻击源资产相似；

3.从攻击过程中使用的钓鱼邮件主题以及关联国内与攻击源资产存在通信的资产归属判断，攻击对象疑似针对国家航空航天领域，属于南亚地区背景的某 APT 组织的战略攻击方向，且航空航天和军事领域是该国近年国家重点战略突破方向。

综合上述因素，对于本次专项攻击归因为南亚地区背景的 APT 组织所为，且主要攻击航空航天领域的多个重点对象。因此，命名本次攻击专项为“九霄行动”。

3.3."暗云风暴"专项

2023 年 8 月 1 日至 3 日，境外 APT 组织疑似利用国内数字化管理平台漏洞，对国内云数字化的政务、大数据中心、交通、医疗、贸易等行业的 80 多个高价值资产展开定向攻击。攻击对象集群空间测绘，并做聚合共性分析发现，96.20%被确定的攻击对象部署国内某云数字化管理平台，51.28%被确定的攻击对象部署于云厂商。

对攻击专项进行互联网攻击链路复盘分析，复现攻击者利用 3 个漏洞利用攻击资产和 5 个特马远控攻击节点对国内 80 多个 IP 攻击对象的攻击路线和模糊原始攻击时间点。

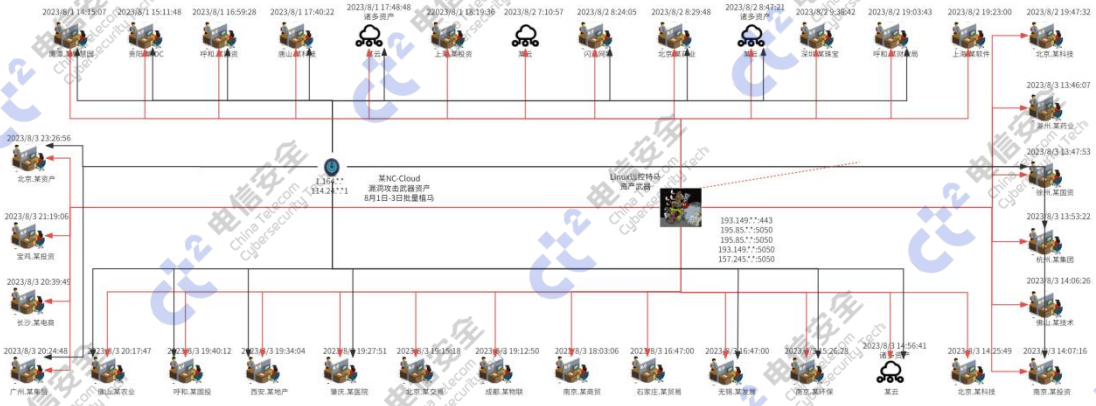


图-互联网攻击链路

除了 80 多个确认植入远控特马的攻击对象外，还发现攻击者对另外 53 个国内资产进行相同的漏洞利用攻击。虽然目前没有掌握这些被漏洞利用攻击的资产是否已经被植入远控

地址：北京市东城区朝阳门北大街 19 号 4 层
网址：www.ctct.cn
电话：400-925-9120

特马，但也说明它们属于攻击者的预定攻击对象，不排除被植入未掌握情报的远控特马的可能，涉及云数字化 ZF 部门、交通、科研、能源等行业。

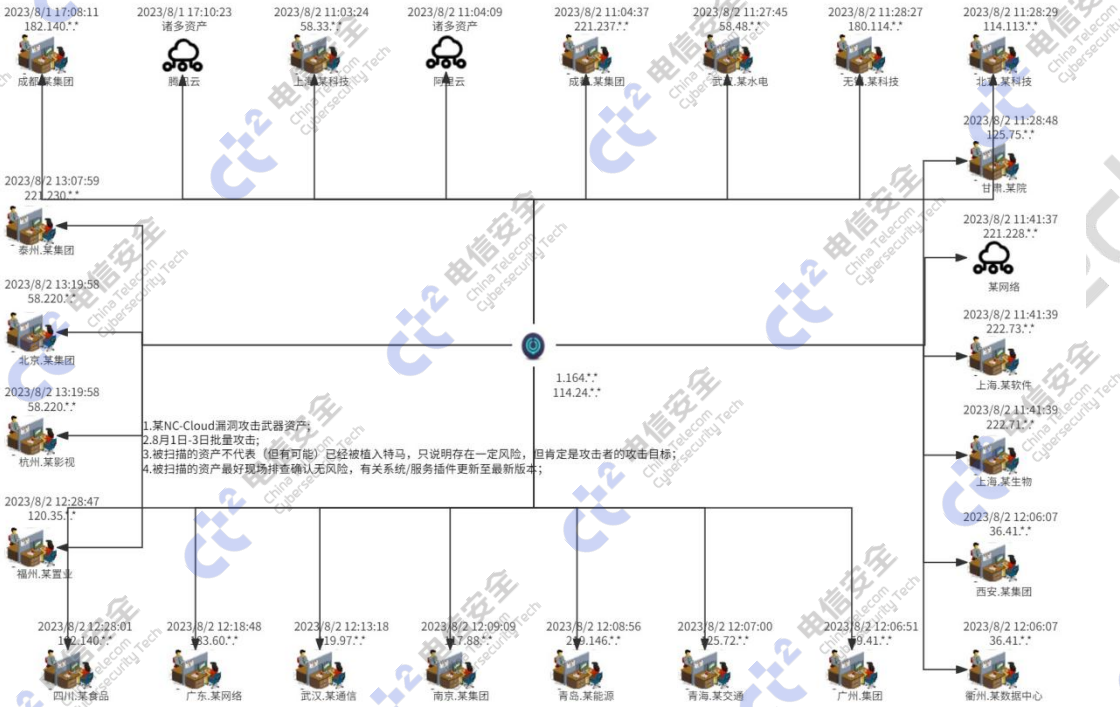


图-漏洞利用攻击链路

挑选 2 个风险系数较高的攻击对象做综合风险分析，同时也抽取北京、广东两个攻击对象做攻击源复原案例分析。

关键指标 \ 攻击对象	`暗云风暴`行动	广东某攻击对象	北京某攻击对象
风险系数星值	★★★★★	★★★★	★★★
高价值威胁风险权值	149511	2150	1330
高价值数据风险权值	22745115	339021	234361
高价值数据泄漏风险权值	8474269	175819	85074
高价值指令数据传输风险权值	14270846	163202	129287
高价值威胁风险系数	386.66	46.36	36.46
高价值数据风险系数	4,769.18	582.26	484.11
高价值数据泄漏风险系数	2,911.05	419.31	291.67
攻击活动周期（天）	40	38	21
威胁等级系数	5	5	5

地址：北京市东城区朝阳门北大街 19 号 4 层
网址：www.ctct.cn
电话：400-925-9120

高价值综合风险系数（预警值>100）	40,534.45	5,429.65	4,166.2
数据泄漏风险占比	37.25±%	51.86±%	36.30±%
交叉感染木马量	1	1	1

表－攻击对象关键风险数据项梳理

攻击者在 8 月 1 日至 3 日，共使用 10 个攻击资产迅速成功控制 80 多个国内攻击对象，攻击威胁风险指数爆发式拉升，并于 8 月 6 日进入峰值，随后进入长期平稳状态。

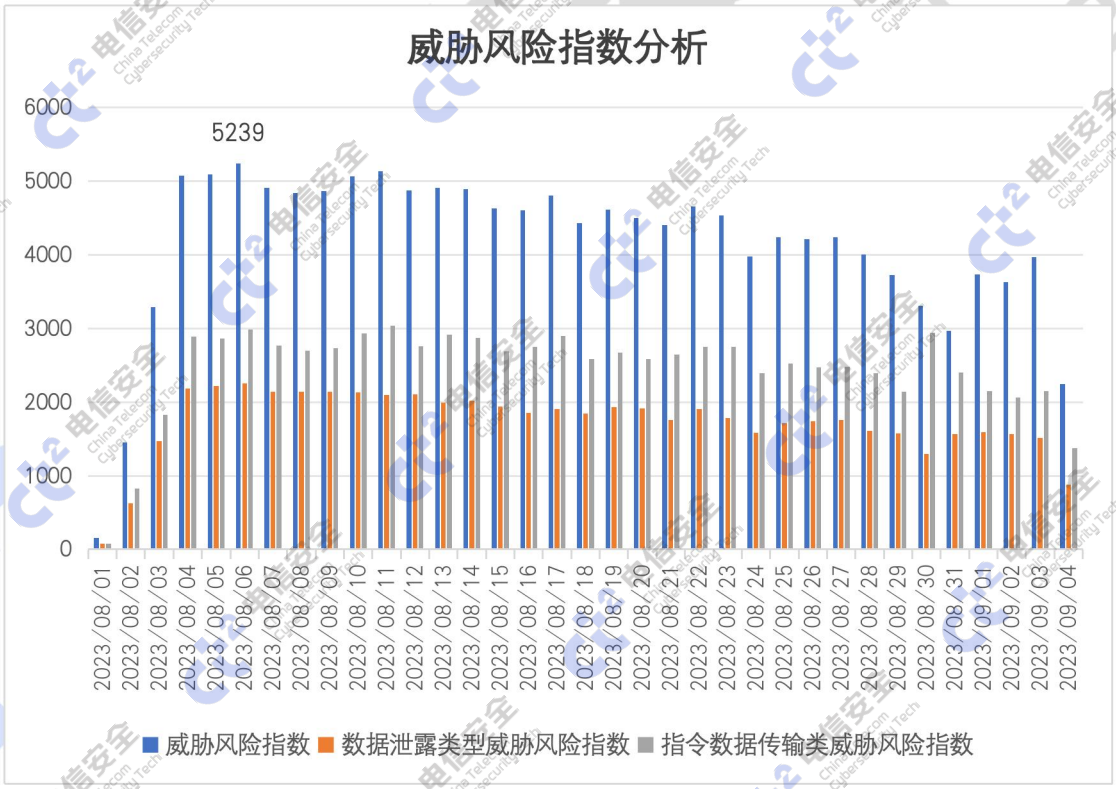


图-威胁风险指数分析

数据风险指数趋势与威胁风险指数基本吻合，在整个攻击专项过程中指令数据传输风险指数高于数据泄漏风险指数，说明可能还没有存在大规模数据泄露现象，也有可能这批攻击对象将作为后期攻击国内重要目标的跳板。

地址：北京市东城区朝阳门北大街 19 号 4 层
网址：www.ctct.cn
电话：400-925-9120

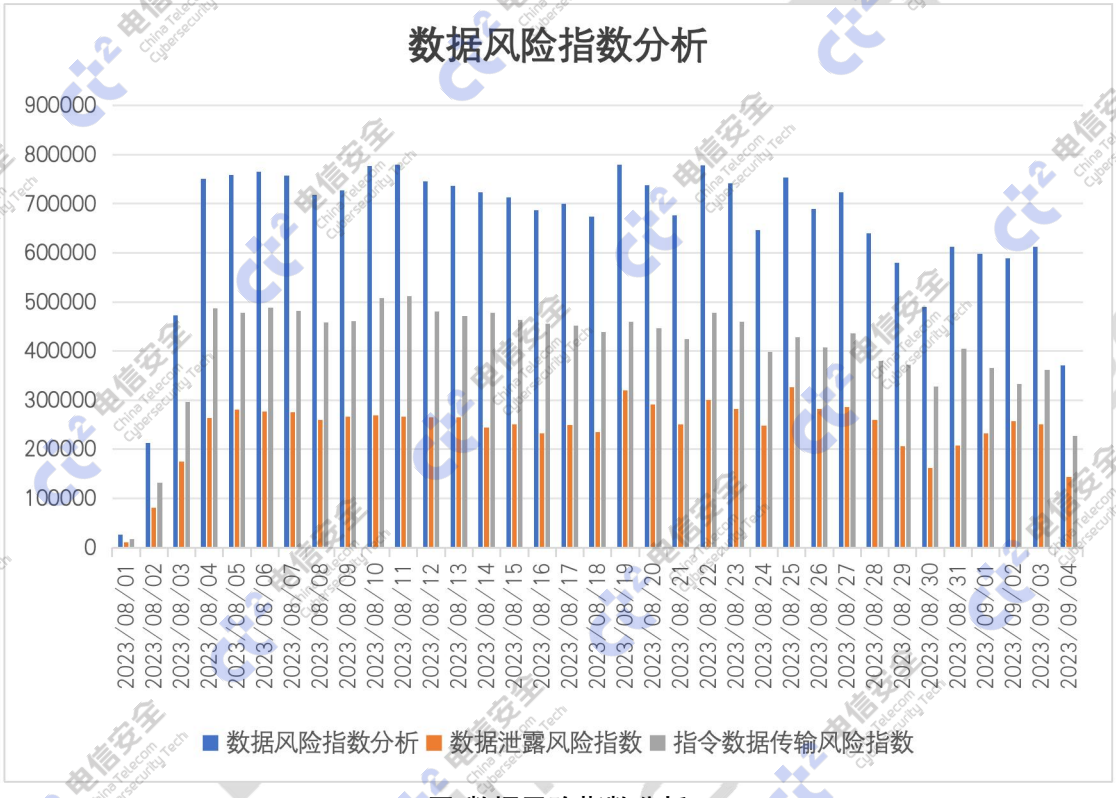


图-数据风险指数分析

结合本次专项攻击的攻击对象特征、攻击手法、攻击者归属等属性，命名本次 APT 攻击专项为“暗云风暴”。“暗云风暴”与“尼格风暴”相似性如下：

使用的 IP 资产与“尼格风暴”行动中极其相似，包括：

- 相同的证书信息；
- 证书时间相近；
- 相同不常见端口和返回相同响应包；
- 相同 TLS 配置指纹；

图-资产指纹比对

地址：北京市东城区朝阳门北大街 19 号 4 层
网址：www.ctct.cn
电话：400-925-9120

本次攻击使用高度免杀的 Linux 特马与尼格风暴中的一致，同样是具备相同扫描功能的特马，同时样本编译信息中 git 版本控制系统时间为 2023-07-10T04:44:20Z，这点也与“尼格风暴”中的特马一致，都在凌晨时分。

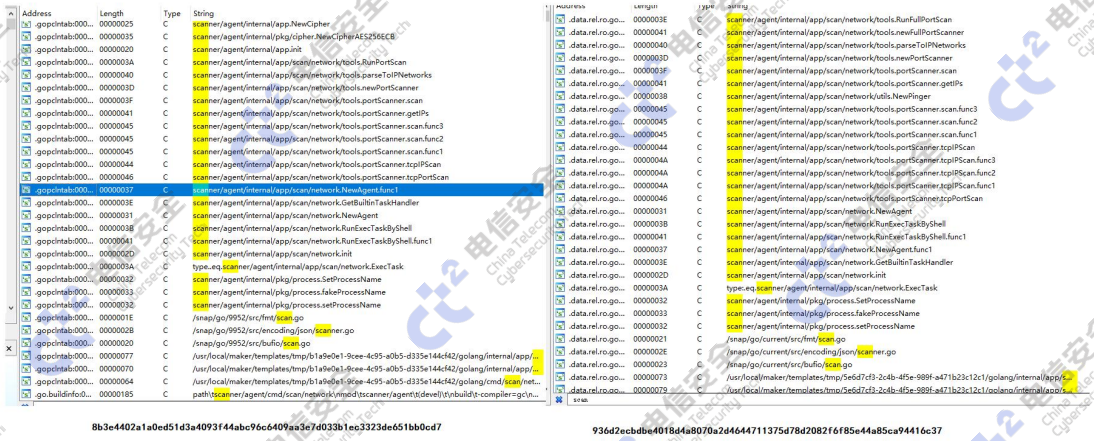


图-样本基因比对

根据对本次攻击专项中失陷机器端口服务统计发现，多为国内数字化管理平台，所以猜测本次攻击利用该数字化管理平台远程执行漏洞作为一阶段植入手段，和“尼格风暴”中批量使用某防火墙漏洞如出一辙。

3.4."丝绸风暴"专项

2023 年 10 月 17 日前后，境外 APT 组织疑似利用某安全设备远程命令执行漏洞对国内多个攻击对象展开网络攻击专项。攻击者在 2023 年 10 月 17 日至 12 月 15 日期间，利用相同攻击手法和攻击资产，攻击了包括外贸、互联网平台供应链、交通、船舶、政府部门等行业的 30 余项高价值企业资产。攻击过程使用的境外攻击资产画像特征，初步判断为一次专项攻击。

从攻击对象特征、攻击链路、攻击对象案例等方面对网络攻击对象进行深层次分析挖掘。本次攻击涉及重点攻击对象有多个政务部门和研究设计院，以及批量高校、互联网设备供应商、医院等行业单位。

对攻击专项进行互联网攻击链路复盘分析，复现攻击者利用 1 个漏洞利用攻击资产和 1 个特马远控攻击节点攻击国内 10 多个 IP 攻击对象的攻击路线和模糊原始攻击时间点。

地址：北京市东城区朝阳门北大街 19 号 4 层
网址：www.ctct.cn
电话：400-925-9120

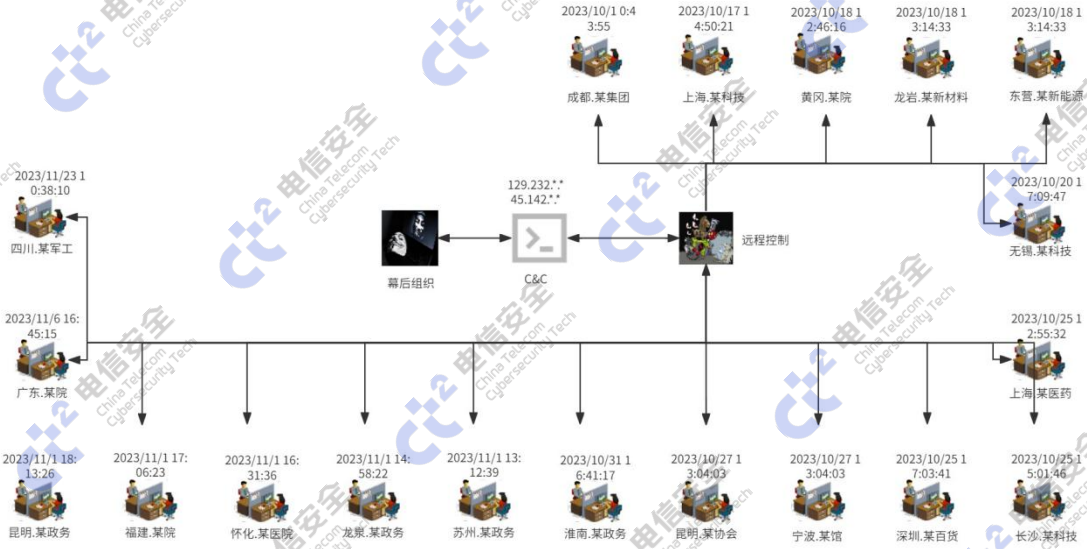


图-互联网攻击链路复盘

除了确认回连远控特马资产的攻击对象外，还发现攻击者对另外 10 多个国内资产在 8 月 16 日至 12 月 15 日在同源木马仓储地下载木马。

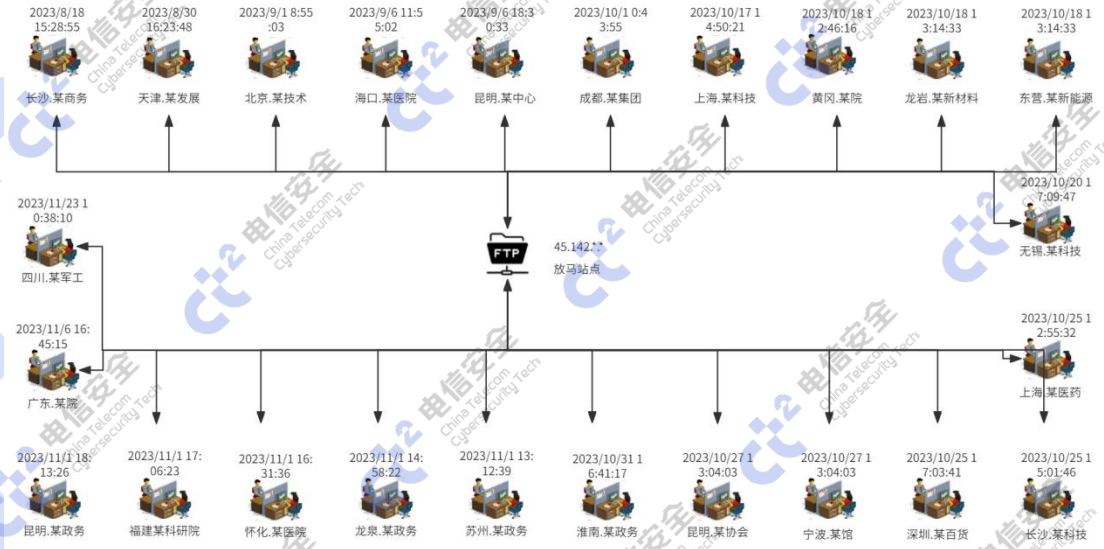


图-木马下载链路还原

挑选 2 个风险系数较高的攻击对象做综合风险分析。

关键指标 / 攻击对象	本次专项攻击	某 JG 攻击对象	淮南某攻击对象
风险系数星值	★★★★★	★★★★★	★★★★
高价值威胁风险权值	46246	5180	3376
高价值数据风险权值	6437500	669749	444227

地址：北京市东城区朝阳门北大街 19 号 4 层
网址：www.ctct.cn
电话：400-925-9120

高价值数据泄漏风险权值	3552689	443719	227012
高价值指令数据传输风险权值	2884811	226075	217215
高价值威胁风险系数	215.04	117.72	58.10
高价值数据风险系数	2537.22	818.38	666.50
高价值数据泄漏风险系数	1884.85	666.12	476.45
攻击活动周期（天）	92	80	18
威胁等级系数	5	5	5
高价值综合风险系数（预警值>100）	24105.55	8,231.1	6095.25
数据泄漏风险占比	55.19%	66.25%	51.10%
交叉感染木马量	1	1	1

表 - 攻击对象关键风险数据项梳理

各项风险指标数据表明，整个攻击专项行动期间，对国内攻击对象存在较大的综合风险同时个别攻击对象可能存在内网横移和数据泄漏可能，且攻击者会对高价值攻击对象进行反复入侵感染木马和利用 kscan 工具入侵内网。

攻击者在 8 月 16 日至 12 月 15 日利用同源木马仓储站点展开攻击，其间成功向 30 多个国内攻击对象投毒，攻击威胁风险指数在 11 月 10 日爆发式拉升，并于 12 月 20 日进入峰值，12 月 22 日进入处置状态。

地址：北京市东城区朝阳门北大街 19 号 4 层
网址：www.ctct.cn
电话：400-925-9120

图-威胁风险指数分析

数据风险指数趋势与威胁风险指数基本吻合，在整个攻击专项过程中数据泄漏风险指数略高于指令数据传输风险指数，但在 11 月 10 日数据泄漏风险指数明显高于指令数据传输风险指数，说明该时间段可能有攻击对象存在内网横移和数据泄露的现象。

地址：北京市东城区朝阳门北大街 19 号 4 层
网址：www.ctct.cn
电话：400-925-9120

图-数据风险指数分析

对本次攻击中涉及的 30 个攻击对象 IP 资产进行空间测绘分析，86.11%比例的攻击对象都部署了国内某厂商防火墙产品平台。结合本次攻击专项的攻击对象特征、攻击手法、攻击时间、攻击者归属等属性，命名本次 APT 攻击专项为“丝绸风暴”。

历史线索分析对比了解，“丝绸风暴”与“尼格风暴”两个专项行动使用特马基因比对一致。此外，在 2023 年 8 月 18 日的同源木马仓储站点下载木马关联事件中，攻击对象是被利用与“暗云风暴”专项相同的漏洞攻击，且时间与“暗云风暴”专项相近，攻击资产指纹高度重合。因此，判断“尼格风暴”、“暗云风暴”、“丝绸风暴”先后三个专项攻击属于同一幕后组织所为。

地址：北京市东城区朝阳门北大街 19 号 4 层
网址：www.ctct.cn
电话：400-925-9120

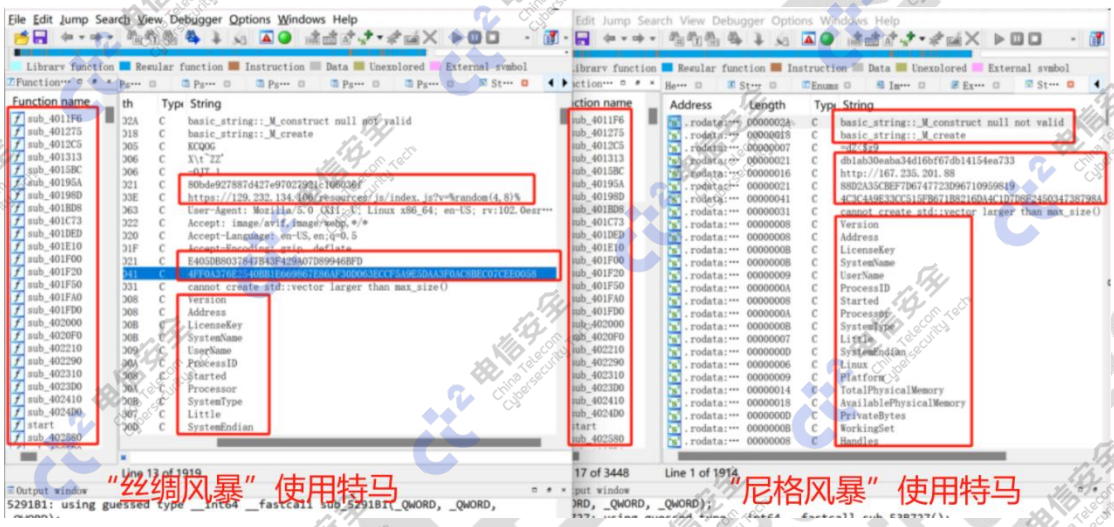


图-特马基因片段比对

3.5."军刀行动"专项

在 2023 年 10 月 6 日至 2024 年 2 月 2 日，有境外 APT 组织对国内 JG 行业展开专项窃密攻击活动。攻击者疑似通过钓鱼邮件方式渗透到攻击对象企业内部网络。专项攻击各项风险指标如下：

关键指标——攻击对象	专项 APT 攻击
风险系数星值	★★★★★
高价值威胁风险权值	5451
高价值数据风险权值	3703012
高价值数据泄漏风险权值	3140649
高价值指令数据传输风险权值	562363
高价值威胁风险系数	45.42
高价值数据风险系数	1,924.32
高价值数据泄漏风险系数	1,772.18
攻击活动周期（天）	126
威胁等级系数	5

地址：北京市东城区朝阳门北大街 19 号 4 层
网址：www.ctct.cn
电话：400-925-9120

高价值综合风险系数（预警值>100）	19,339.6
数据泄漏风险占比	84.81%
交叉感染木马量	1

威胁狩猎分析，攻击者的专项攻击始于 2023 年 10 月 6 日疑似对具有 JG 背景的某机器人自动化研究生产企业攻击，2023 年 10 月 24 日疑似对某科研机构攻击，11 月 23 日疑似对某汽车制造企业攻击，后续则对一系列 JG、政企和边贸单位展开攻击。

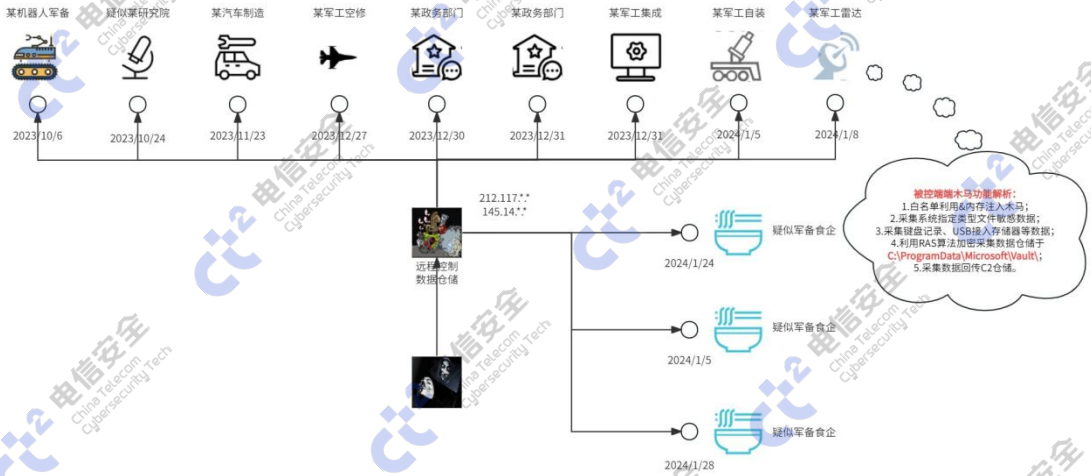


图-专项行动互联网攻击链路还原

终端攻击链路复原结果分析，攻击者在攻击过程中追求无人为干预下长期性潜伏和重要数据信息窃取。攻击者利用钓鱼邮件方式向潜在攻击对象员工投递木马母体，诱导终端加载运行木马，开始执行系列终端操作流程如下：

- 创建注册表自启动项，SOFTWARE\Intel\Display\igfxcui\igfxtray\TrayIcon\ShowTrayIcon；
- 白名单利用&内存 dll 注入木马，加载 hccutils.dll，解密释放核心模块；
- 加载旁目录 Crypto 下 ceip_usb.dll、crypto_rsa.dll；
- 采集系统指定类型文件敏感数据；
- 采集键盘记录、截屏、USB 接入存储器等动态数据；
- 调用 crypto_rsa.dll 利用 RSA 算法加密采集数据仓储于 C:\ProgramData\Microsoft\Vault\；

地址：北京市东城区朝阳门北大街 19 号 4 层
网址：www.ctct.cn
电话：400-925-9120

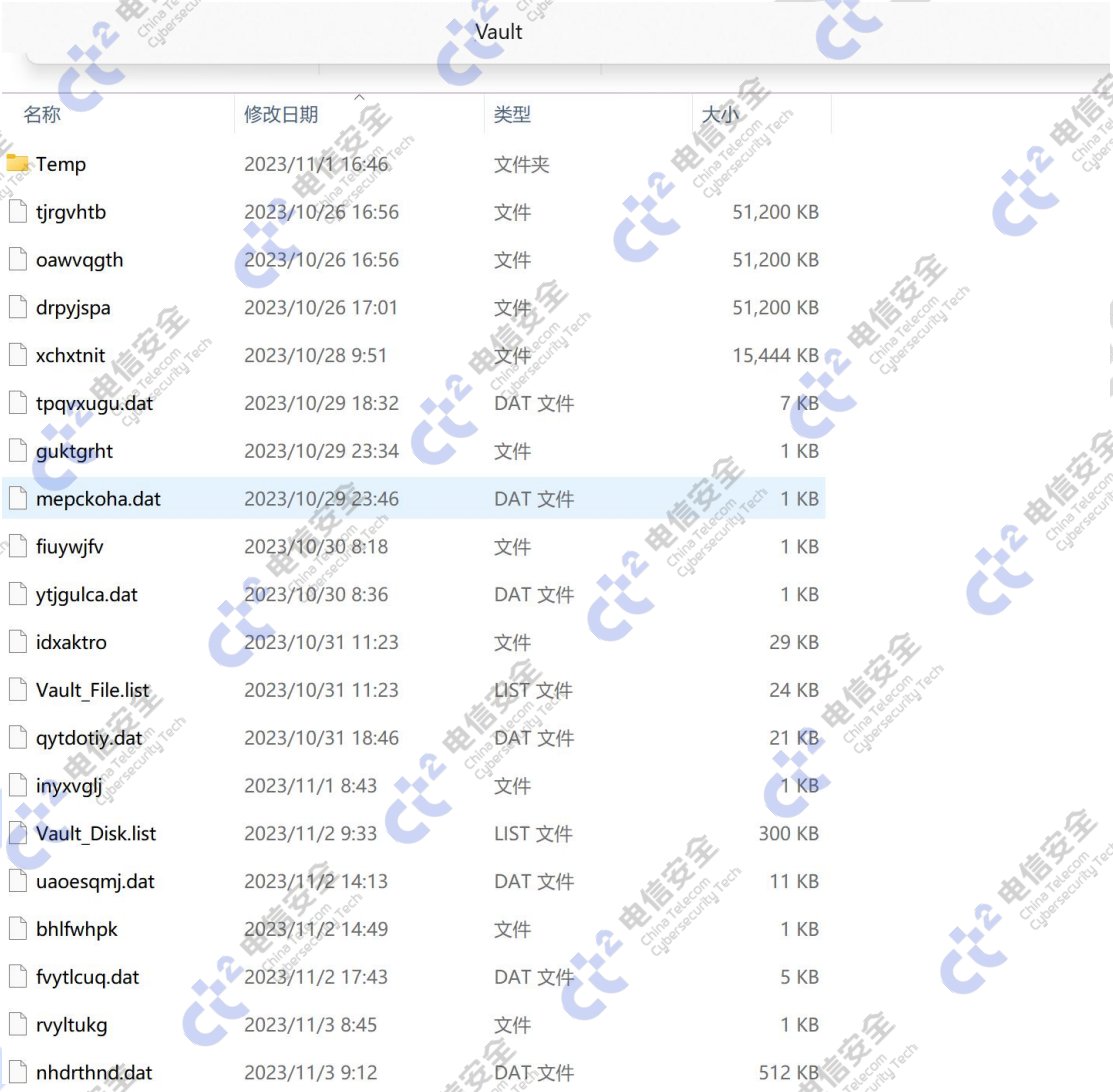


图-Vault 目录采集的加密数据

- 采集数据回传 C2 仓储，目前已监测数十个 JG、科研、边贸等行业的企业存在感染痕迹，且有数据外泄的迹象。

地址：北京市东城区朝阳门北大街 19 号 4 层
网址：www.ctct.cn
电话：400-925-9120

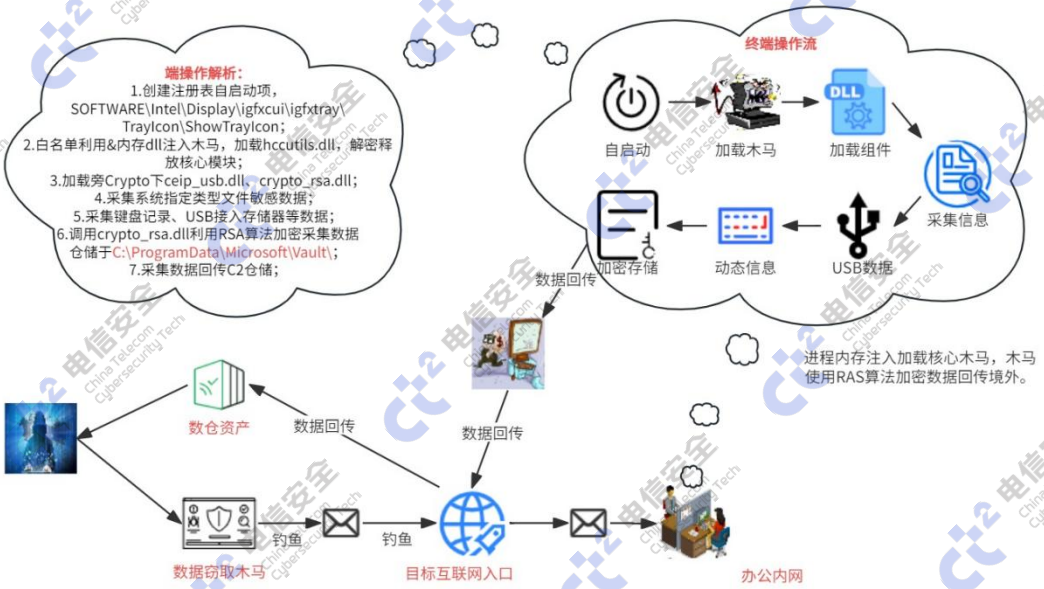


图-攻击事件链路还原

在整个攻击专项中，攻击威胁风险指数峰值存在多波段模式，在 2023 年 12 月 8 日前的波段形态威胁风险指数是由于逐个攻击对象定点攻击模式形成；2024 年 1 月 2 日至 2 月 3 日的密集式风险是因攻击者开始批量攻击 JG 企业且风险未及时发现并清除而形成的。威胁风险指数如下：

地址：北京市东城区朝阳门北大街 19 号 4 层
网址：www.ctct.cn
电话：400-925-9120

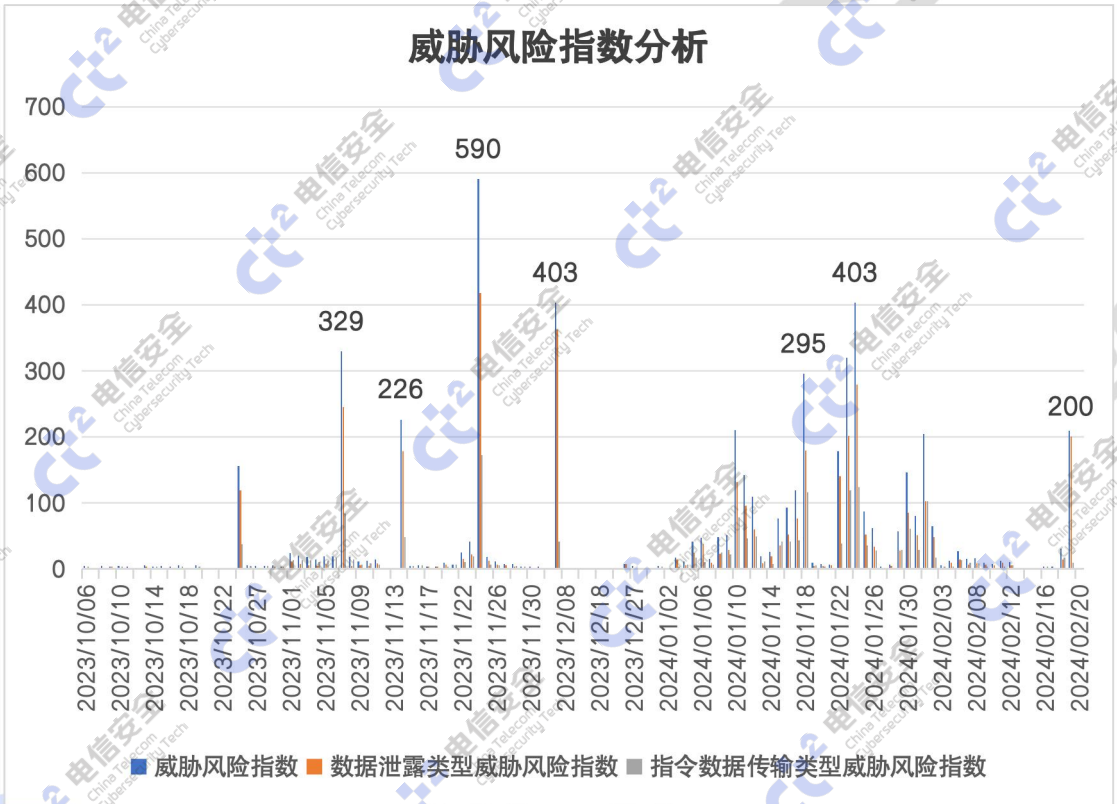


图-威胁风险指数分析

从数据风险指数看，指数趋势基本与威胁风险指数一致，在 2023 年 12 月 8 日前的攻击事件中数据泄露风险比较明显，但没有形成持续泄露模式，初步逆向估算可能造成 1.83-9.15G 的数据泄露；2024 年 1 月 2 日至 2 月 3 日的数据泄露风险比较持续性，但峰值相比不明显，其间攻击对象可能造成 1.30-6.51G 的数据泄露。从整个专项行动数据风险评估，数据泄露风险占比 84.81%，符合信息窃取目的的攻击特征。数据风险指数分析如下：

地址：北京市东城区朝阳门北大街 19 号 4 层
网址：www.ctct.cn
电话：400-925-9120

图-数据风险指数分析

如上攻击对象明细显示，攻击者有明显针对 JG 行业攻击的倾向，其次是边贸（攻击影响不明显）、通信、科研与政务单位，且攻击并没有主要分布在东部沿海省份，而是 JG 企业较为集中的省份，例如湖北、陕西、辽宁、四川等省份。

地址：北京市东城区朝阳门北大街 19 号 4 层
网址：www.ctct.cn
电话：400-925-9120

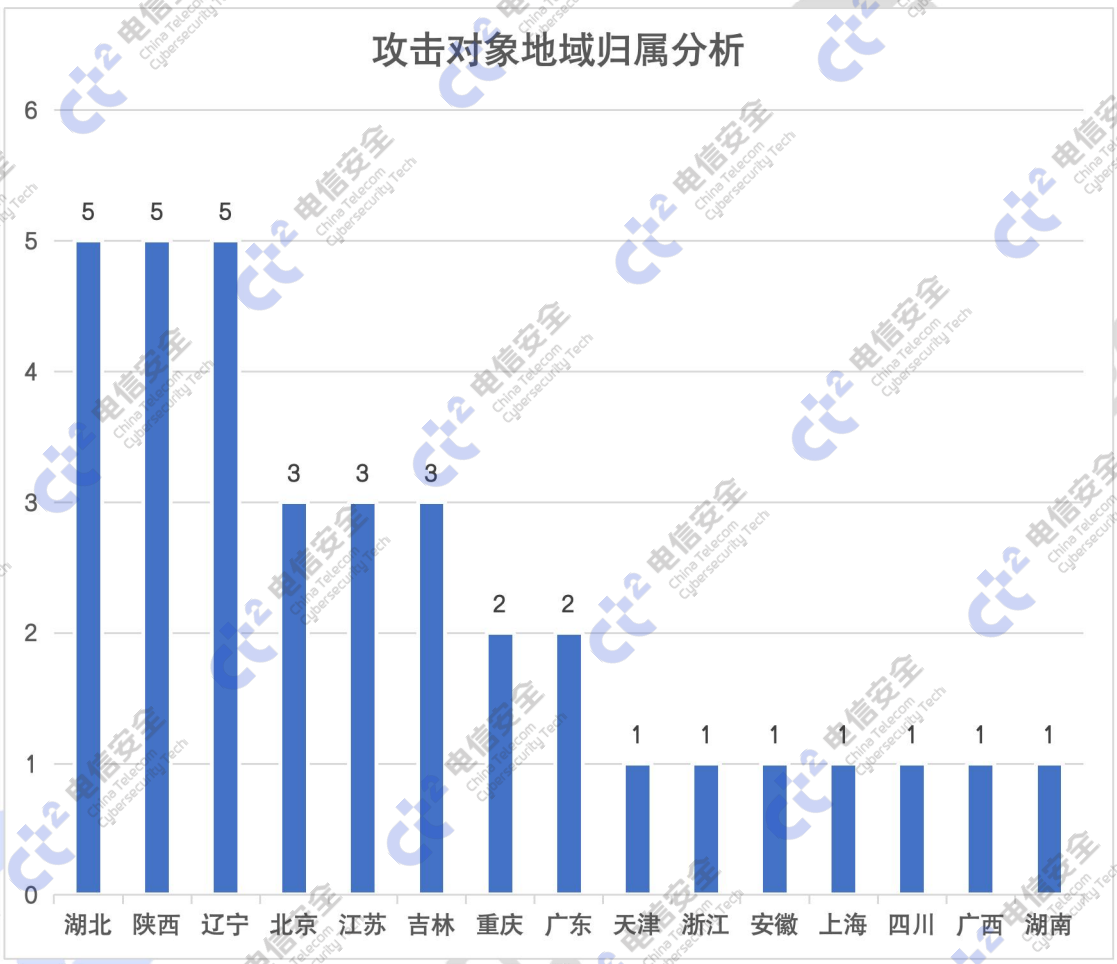


图-攻击对象各省统计

对本次专项行动的攻击资产、武器库、目的、攻击对象、地域分布等多维度做聚合比对分析攻击者幕后归属。

- 攻击资产上，出现的协议指纹和数字证书的细节比对，与 Darkhotel 组织历史攻击资产高度相似；
- 攻击对象上，本次专项涉及攻击对象主要是 JG、边贸、通信、科研与政务等行业资产，
- 地域分布上，本次专项涉及的边贸行业攻击对象，都属于东北亚地区关联的边贸，与 Darkhotel 组织长期战略目标吻合。
- 武器库和目的上，攻击者比较追求无人为干预下长期性潜伏和重要数据信息窃取，与 Darkhotel 组织长期物理隔离传播渗透并窃取数据的目的吻合；

地址：北京市东城区朝阳门北大街 19 号 4 层
网址：www.ctct.cn
电话：400-925-9120

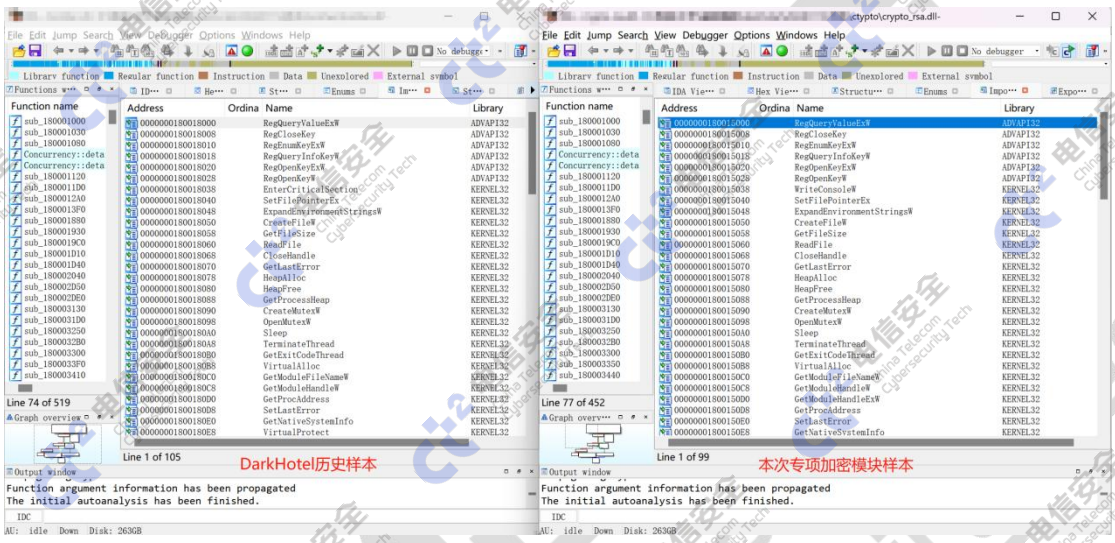


图-样本基因片段比对

因此，综合各项分析判断，本次针对国内 JG、边贸、通信、政务、科研等行业攻击的专项行动，其幕后归属疑似为东北亚地区 Darkhotel 组织，并命名本次专项攻击为“军刀行动”。

3.6. Mallox 勒索团伙利用 1day 漏洞攻击专项

在 2023 年 11 月 28 日至 12 月 8 日，境外高级勒索团伙疑似利用某 OA 管理系统、某审批管理系统、某资源管理系统的漏洞，攻击中国境内能源、高新科技、数据中心、金融和生物制药等行业的 20 多个企业/部门，植入后门后尝试内网横移窃取数据并投递 Mallox 勒索木马加密数据，且已有多个攻击对象被数据加密勒索，初步估算整个专项攻击可能造成 50+G 的数据泄露。

从涉及国内的 20 多个攻击对象关联分析判断，勒索团伙先后利用国内三个产品（某 OA 管理系统、某审批管理系统、某资源管理系统）的漏洞进行攻击，上传 webshell 后门，随后部署内网代理和内网横移攻击。

产品名称	漏洞复现披露报告	漏洞披露时间
某 OA 管理系统	https://github.com/wy876/POC/blob/f384c0d48494f5d5780db0e88cde95f4be201c3a	2023/11/16
某审批管理系统	https://github.com/MD-SEC/MDPOCS/tree/main	2023/11/09
某资源管理系统	https://github.com/wy876/POC/blob/f384c0d48494f5d5780db0e88cde95f4be201c3a/	2023/11/29

终端日志排查验证，勒索团伙使用的漏洞属于 11 中下旬在互联网披露，且漏洞披露时

地址：北京市东城区朝阳门北大街 19 号 4 层
网址：www.ctct.cn
电话：400-925-9120

间与被勒索团伙利用的时间差最长 22 天，最短只有 3 天，充分说明勒索团伙具备漏洞武器库收集和补充能力。

产品名称	漏洞披露时间	勒索团伙初始利用时间	披露与使用时间差
某 OA 管理系统	2023/11/16	2023/12/05	19 天
某审批管理系统	2023/11/09	2023/12/01	22 天
某资源管理系	2023/11/29	2023/12/02	3 天

勒索团伙整个专项行动利用上述 3 个漏洞成功向 20 多个攻击对象植入 webshell 后门，并根据攻击对象价值评估内网横移攻击优先级排期。

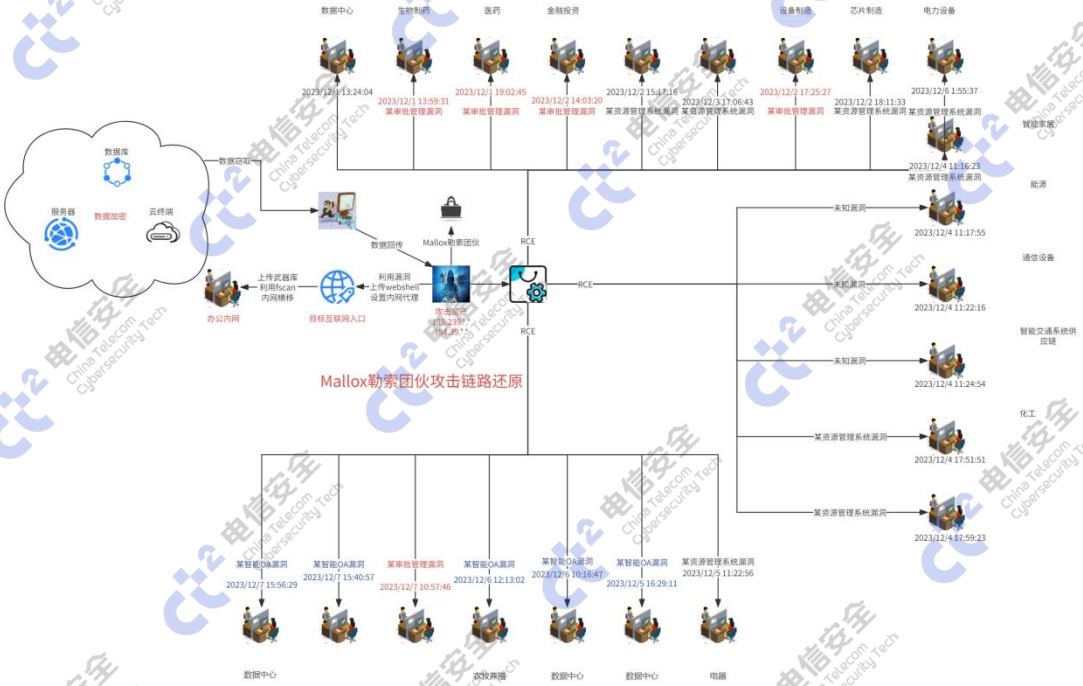


图-互联网攻击链路还原

如上攻击对象明细显示，勒索团伙攻击者在植入后门环节上并没有明显针对行业对象（覆盖数据中心、高新科技、能源、通信、金融和生物制药等），但在内网横移攻击环节，攻击者会重点倾向数据中心和高新科技企业，因为潜在敲诈对象的业务运营数字化和可支付巨额赎金的概率是勒索团伙重点评估维度。

地址：北京市东城区朝阳门北大街 19 号 4 层
网址：www.ctct.cn
电话：400-925-9120

攻击开始时间	攻击对象地区归属	攻击对象省份归属	攻击源IP*	攻击资产地域归属	攻击对象疑似行业归属
2023/12/01 13:59:31	安徽.合肥	安徽	154.39.*.*	新加坡	生物医药
2023/12/04 11:17:55	安徽.合肥	安徽	154.39.*.*	新加坡	能源
2023/12/04 11:22:16	安徽.合肥	安徽	154.39.*.*	新加坡	通信供应链
2023/12/04 11:24:54	安徽.合肥	安徽	154.39.*.*	新加坡	智能交通系统、安全防范系统和网络通讯系统等警务单位供应链
2023/12/06 10:16:47	北京.北京	北京	154.39.*.*	新加坡	数据中心
2023/12/04 09:22:32	福建.宁德	福建	154.39.*.*	新加坡	电力设备
2023/12/01 13:24:04	广东.佛山	广东	154.39.*.*	新加坡	数字化政务、互联网、软件开发、政务系统供应链
2023/12/04 11:16:23	广东.东莞	广东	154.39.*.*	新加坡	智能家居
2023/12/07 15:40:57	广东.东莞	广东	154.39.*.*	新加坡	其他
2023/12/04 17:59:23	广东.佛山	广东	154.39.*.*	新加坡	其他
2023/12/05 16:29:11	广东.佛山	广东	154.39.*.*	新加坡	数据中心
2023/12/06 00:05:06	广东.佛山	广东	185.239.*.*	新加坡	数据中心
2023/12/02 11:22:36	广东.广州	广东	185.239.*.*	新加坡	金融投资
2023/12/02 17:20:10	广东.惠州	广东	185.239.*.*	新加坡	设备制造
2023/12/02 16:10:40	广东.深圳	广东	154.39.*.*	新加坡	其他
2023/12/03 10:52:03	广东.深圳	广东	185.239.*.*	新加坡	芯片制造
2023/12/07 10:57:46	广东.深圳	广东	185.239.*.*	新加坡	其他
2023/12/02 17:41:33	广东.中山	广东	154.39.*.*	新加坡	其他
2023/12/07 15:56:29	湖南.株洲	湖南	185.239.*.*	新加坡	数据中心
2023/12/01 18:43:13	江苏.苏州	江苏	185.239.*.*	新加坡	医药
2023/12/05 11:22:56	江苏.镇江	江苏	154.39.*.*	新加坡	电器
2023/12/02 14:59:09	山东.东营	山东	154.39.*.*	新加坡	其他
2023/12/04 17:51:51	山东.青岛	山东	154.39.*.*	新加坡	化工
2023/12/06 12:13:02	山东.青岛	山东	154.39.*.*	新加坡	农牧养殖
2023/12/07 13:07:40	上海.上海	上海	185.239.*.*	新加坡	其他

表-勒索攻击对象分析

如上攻击链路所述，勒索团伙攻击者成功向攻击对象植入后门后，评估确定对攻击对象内网横移攻击，之后会植入网络代理木马设置网络代理，并上传内网横移武器库（fscan 等扫描工具）和勒索木马套件。攻击者利用 fscan 采集到的资产网络架构和账号信息，重点渗透数据服务器和业务生产服务器，成功获取服务器权限后尝试窃取并回传数据，随后加载运行勒索木马进行数据加密。

地址：北京市东城区朝阳门北大街 19 号 4 层
网址：www.ctct.cn
电话：400-925-9120

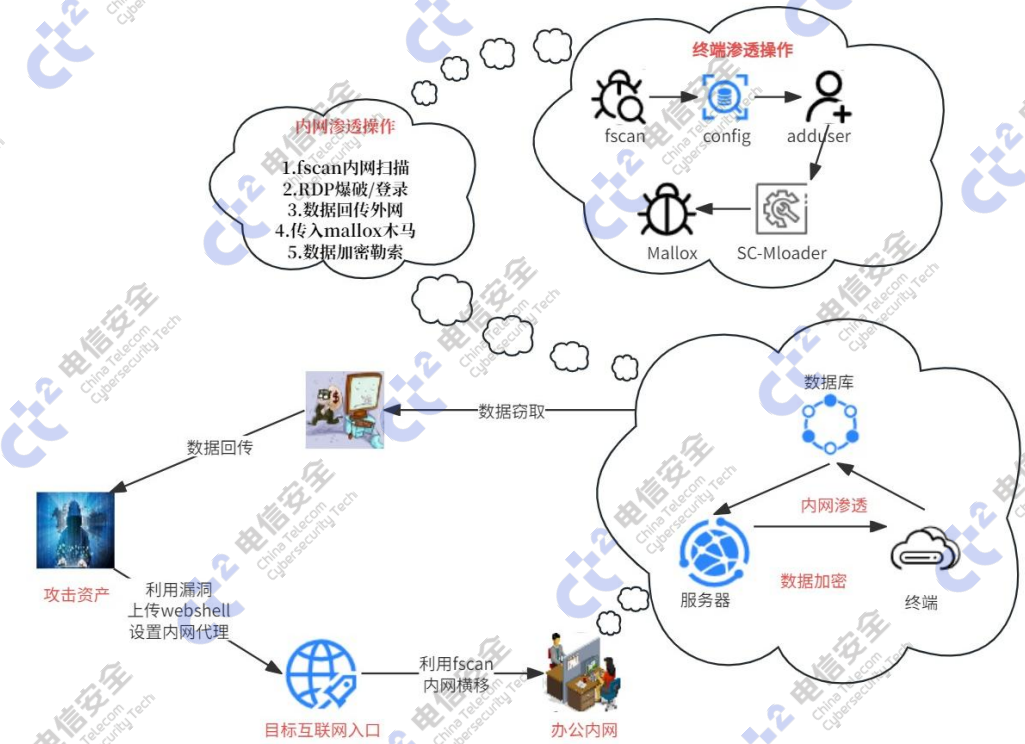


图-Mallox 攻击事件链路还原

挑选 2 个攻击对象做综合风险评估分析，如下各项关键风险数据项梳理：

关键指标 / 攻击对象	勒索专项攻击	某生物攻击对象	某芯片攻击对象
风险系数星值	★★★★★	★★★★★	★★★★
高价值威胁风险权值	8999	6025	1255
高价值数据风险权值	7517511	6415420	438878
高价值数据泄漏风险权值	6936378	6257743	241722
高价值指令数据传输风险权值	581133	157681	197156
高价值威胁风险系数	1124.87	1004.16	313.75
高价值数据风险系数	2,741.80	2532.86	662.47
高价值数据泄漏风险系数	2,633.70	2501.54	491.65
攻击活动周期（天）	8	6	4
威胁等级系数	5	5	5
高价值综合风险系数（预警值>100）	32,541.85	30,222.8	7359.35

地址：北京市东城区朝阳门北大街 19 号 4 层
网址：www.ctct.cn
电话：400-925-9120

数据泄漏风险占比	61.01%	97.54%	55.07%
交叉感染木马量	1	1	1

勒索团伙在整个攻击专项中，攻击威胁风险指数[3]峰值在 12 月 3 日，核实确认为 12 月 2 日新增攻击对象（疑似芯片企业）形成，勒索团队对该攻击对象进行高强度攻击，而 12 月 4 日高威胁风险指数值是因高新增攻击对象量形成。如图 Mallox 威胁日志指数分析：

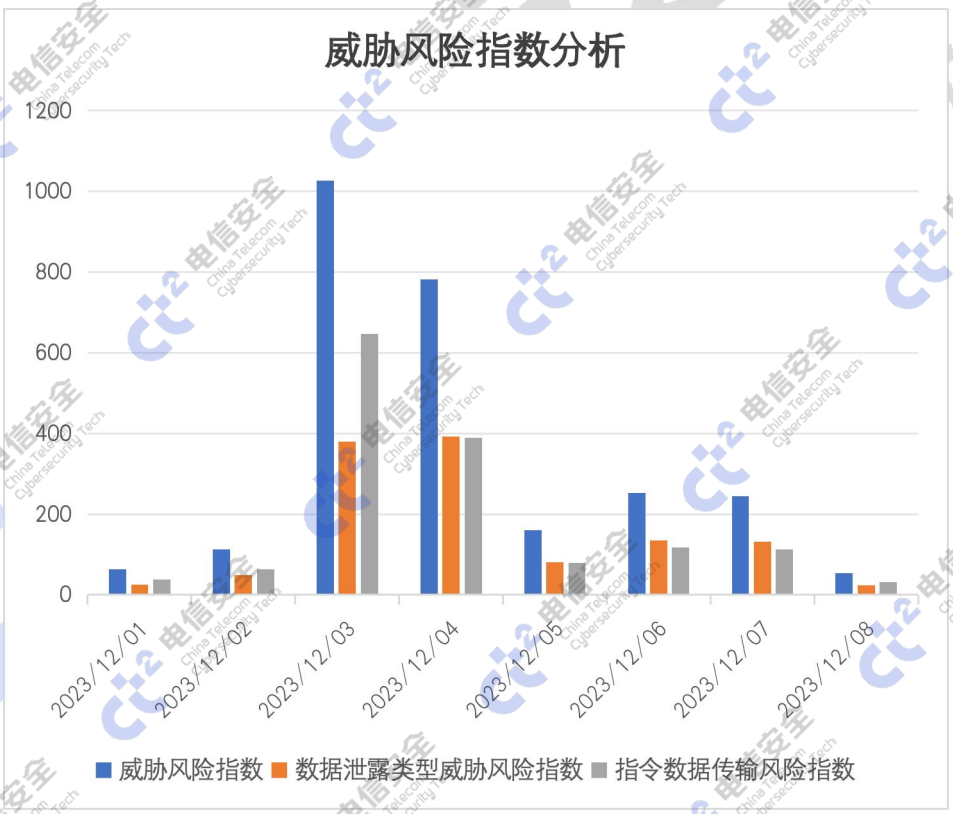


图-威胁风险指数分析

3.7.BlackCat 勒索团伙攻击高质量发展行业专项

在 2023 年 12 月 1 日至 28 日，境外高级勒索团伙通过社工投毒方式，攻击国内高新制造、高质量发展类型企业的十多个资产，植入后门后尝试内网横移窃取数据并投递 BlackCat 勒索木马加密数据，初步估算最高可能造成 10G 的数据泄露，专项攻击风险在 2024 年 1 月 18 日前基本得到清除。

[3] 威胁风险指数：自研专利数据分析模型，威胁风险指数越高，攻击活动越强烈。

地址：北京市东城区朝阳门北大街 19 号 4 层
网址：www.ctct.cn
电话：400-925-9120

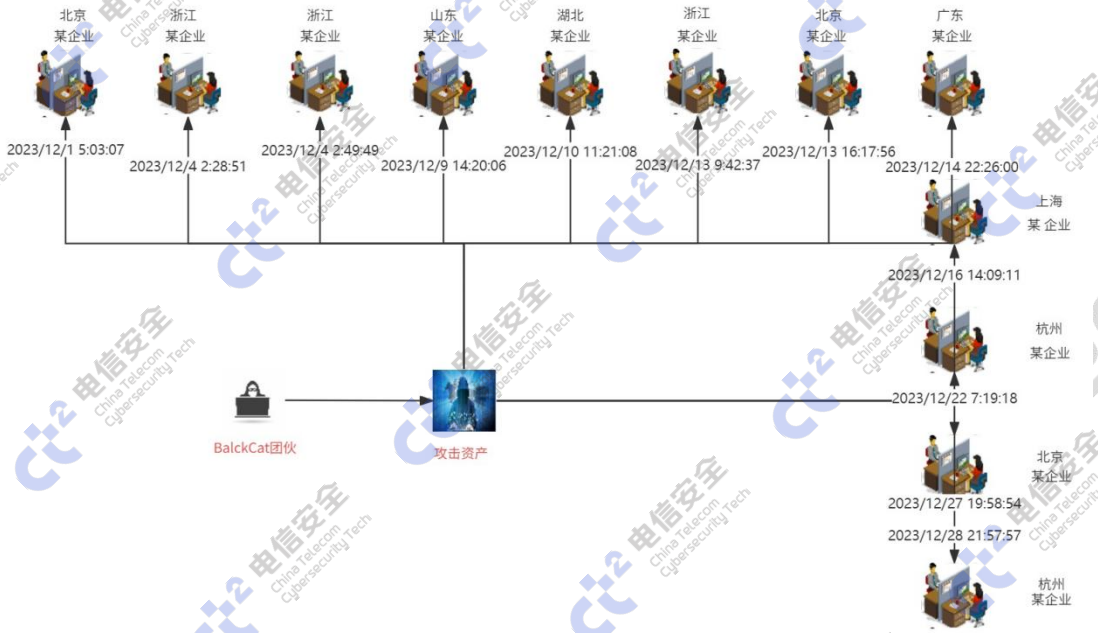


图-BlackCat 专项互联网专攻击链路

通过事件排查和 BlackCat 历史攻击手法还原攻击链路：

- 攻击者通过社工方式向事件企业员工投递原始木马，释放 CobaltStrike 和在 My Pictures 目录下释放 Offline_WinPwn.ps1（WinPwn 等工具）、WinCreds.exe（LaZagne 工具）；

Offline WinPwn.ps1功能解析		
序号	功能明细	备注
1	ADIDNS/LLMNR/mDNS/NBNS欺骗击。	
2	绕过AMSI和UAC。	
3	收集系统信息、浏览器凭证，SessionGopher提取保存在系统中的PuTTY等会话信息，保存到当前目录下创建的LocalRecon、DomainRecon、LocalPrivEsc、Exploitation、Vulnerabilities文件夹。	
4	收集域信息，检查域可能存在的MS17-10、MS-RPRN、CVE-2020-1472等漏洞，域密码喷洒攻击。	
5	漏洞利用，利用系统内核MS16-032、MS16-135、CVE-2018-8120CVE-2019-1215、CVE-2020-0638、CVE-2020-0796、CVE-2021-40449、CVE-2021-34527/CVE-2021-1675漏洞、Juicy-Potato和Printspoofer获取系统级权限。	
6	HandleKatz、WerDump、NanoDump、 Evilginx2转储LSASS提取登录会话密码、哈希和其他认证令牌。	
7	Mimikatz、LaZagne和WebBrowserPassView提取系统密码。	
8	检查Windows系统上可能存在的提权漏洞。	
9	远程加载恶意二进制文件到内存并执行。	
10	添加或删除DNS节点。	
11	可执行自定义Rubeus命令。	
12	清除操作日志	

表-Offline WinPwn.ps1 功能解析

- 利用 STONESTOP 加载由微软签名的 POORTRY 内核模式驱动程序，以结束安全防护进程；
- 利用 Plink 和 Ngrok 搭建内网穿透隧道；

地址：北京市东城区朝阳门北大街 19 号 4 层
网址：www.ctct.cn
电话：400-925-9120

- 利用 Metasploit、WinPwn 工具漏洞利用和内网横移；
- 利用开源工具 Mimikatz、LaZagne、HandleKatz、WerDump、NanoDump 等转储 LSASS 提取登录会话密码、哈希和其他认证令牌和系统密码；
- 利用 Mega.nz 或 Dropbox 用于收集、窃取和下载攻击对象数据；
- 清除操作日志；
- 利用 AnyDesk、Mega sync 和 Splashtop 做数据回传；
- 执行勒索木马，使用 AES 或 ChaCha 和 RSA 算法对数据进行加密。

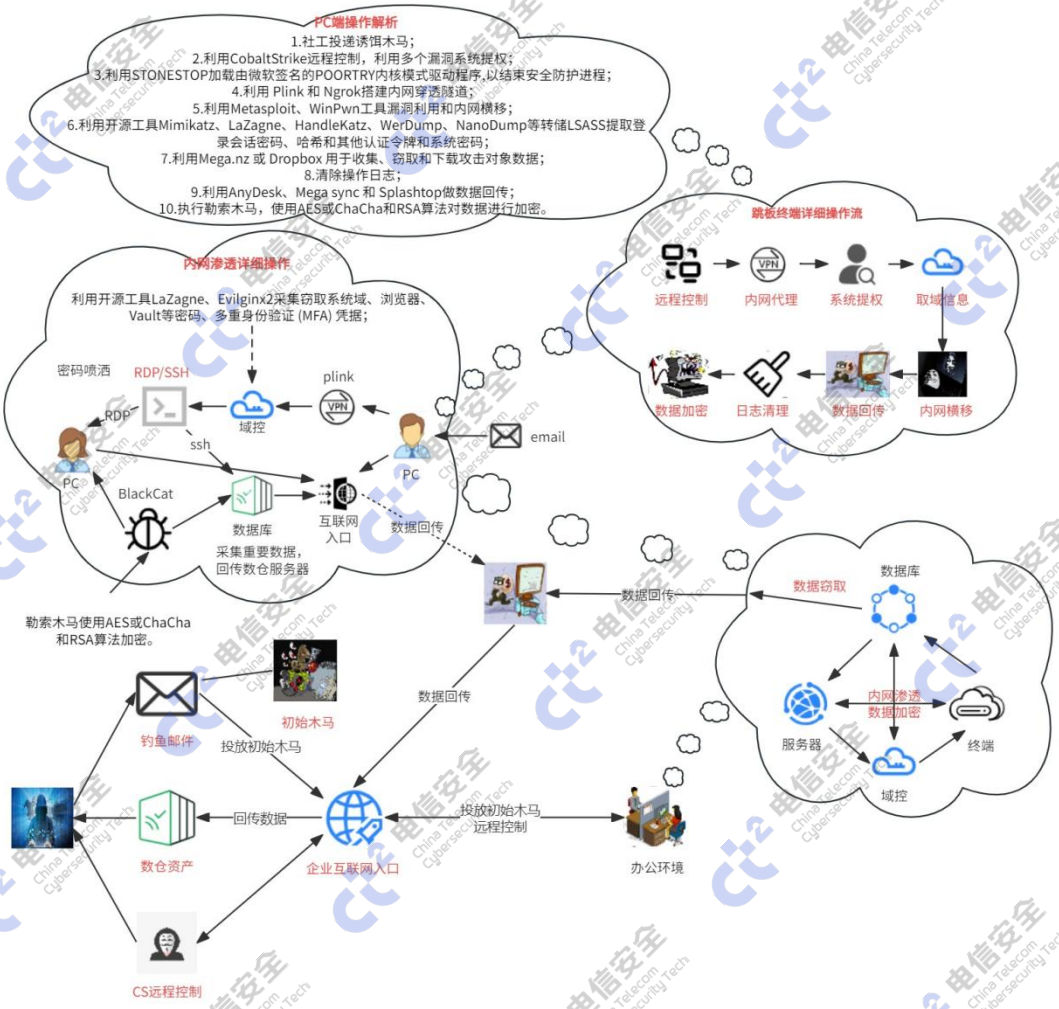


图-BlackCat 攻击事件链路画像

持续对 BlackCat 团伙做攻击威胁狩猎追踪发现，2023 年 12 月 1 日至 28 日期间对国内十多个大型高新制造、高质量发展类型企业展开专项攻击，并可能造成数据泄漏风险。挑选本次专项攻击的 2 个攻击对象做各项风险指标如下：

关键指标 / 攻击对象	勒索专项攻击	山东某攻击对象	浙江某攻击对象
风险系数星值	★★★★★	★★★★★	★★★★

地址：北京市东城区朝阳门北大街 19 号 4 层
网址：www.ctct.cn
电话：400-925-9120

高价值威胁风险权值	5679	3323	1145
高价值数据风险权值	2518906	1828708	369852
高价值数据泄漏风险权值	1857272	1394029	281177
高价值指令数据传输风险权值	661634	434679	88675
高价值威胁风险系数	126.2	332.3	143.12
高价值数据风险系数	1587.10	1352.29	608.15
高价值数据泄漏风险系数	1362.81	1180.69	530.26
攻击活动周期（天）	45	10	8
威胁等级系数	5	5	5
高价值综合风险系数（预警值>100）	15,605.55	14376.4	6,447.65
数据泄漏风险占比	73.73%	76.23%	76.02%
交叉感染木马量	1	1	1

从威胁风险指数角度评估，BlackCat 团伙的攻击威胁风险状态呈明显的波次型攻击，各攻击事件造成的威胁风险明显区分，具有同源排期逐个攻击的特点，也符合社工突破企业内网的攻击特点。整个专项攻击周期的威胁风险指数峰值于 2023 年 12 月 17 日对山东某攻击对象攻击形成。

图-威胁风险指数分析

地址：北京市东城区朝阳门北大街 19 号 4 层
网址：www.ctct.cn
电话：400-925-9120

数据风险指数趋势与威胁风险指数基本相同，在 2023 年 12 月 17 日峰值期间，山东某攻击对象可能造成 6.64G 的数据泄露，整个专项行动最高可能造成 10G 的数据泄露。

图-数据风险指数分析

4.2024 年国内安全威胁发展预测

根据电信安全水滴实验室风险监测数据对比发现，2023 年的 APT 攻击威胁态势比 2022 年严峻，由于国际局势的纷繁复杂，各方利益与矛盾纷繁交错，网络战争的进一步发展，2024 年的 APT 攻击威胁将比 2023 年更为严峻，同时也将面临本土化安全设备或云办公系统通用漏洞的批量化攻击、上游供应链攻击、非传统模式攻击或 APT 与勒索双模式结合攻击和数据外泄等风险。

4.1.APT 攻击行业趋势量变

从 2023 年国内 APT 事件的攻击频率评估，当前国内面临 APT 攻击的风险依次是来自东南亚、南亚、台海、东北亚、东欧、欧美等地区，但真实的高风险度不能单纯地依托攻击频率，更应该从攻击手法复杂度、发现攻击难易度、攻击对象、攻击目的、造成损失/影响等多维度评估。

综合多维度评估，2023 年受 APT 攻击威胁较大的行业是数字化政务、JG、GF、高新科技（通信：5G、卫星通信、量子通信、骨干路由、大型计算，芯片：设计、制造、GPU，自动化：大型制造：船舶、高铁、机器人，新能源：能源存储、新材料研发）、能源系统、

地址：北京市东城区朝阳门北大街 19 号 4 层
网址：www.ctct.cn
电话：400-925-9120

金融系统、教育系统、交通系统。

从大方向预测，2024 年的 APT 攻击行业趋势基本与 2023 年一致，但细分行业可能会向数字化政务、JG、GF、智能计算、智能电控、智能交通等新质生产力行业拓展。

4.2. APT 定向攻击继续拓展通用漏洞批量化攻击

通用漏洞批量化攻击分析				
开始漏洞出现时间	2023/11/30	结束漏洞利用时间	漏洞名称及关联产品	攻击对象数量
2022年HW在野0day	2022/11/16	2023/08/18	某NC防火墙	53
2023年4月	2023/05/23	2023/08/30	某安全产品管理平台	5
2023年7月	2023/08/01	2023/08/03	某NC-Cloud	89
2023年8月	2023/09/06	2023/12/06	某WS防火墙	4
2023年10月	2023/10/17	2023/12/15	某S防火墙	36
2023年10月	2023/11/23	2024/01/05	某OA系统	16
2023年11月	2023/11/29	2023/11/30	某云匣子	7
2023年11月	2023/11/30	2023/12/07	某审批管理系统	7
2023年11月	2023/12/02	2023/12/05	某资源管理系统	8
2023年12月	2023/12/02	2024/01/08	某办公软件	11
2023年12月	2024/01/03	2024/01/03	某安全网关	1

表-通用批量化攻击分析

监测统计，境外 APT 组织在 2023 年利用通用漏洞批量化攻击共记 11 次，漏洞涉及 6 个互联网办公软件/系统厂商和 5 个安全厂商的产品，造成 237 个国内资产因此失陷，占 2023 年国内 APT 攻击事件资产的 27.21%，且攻击密度集中在下半年，第 4 季度新漏洞利用尤为频繁。这说明针对国内 APT 攻击威胁的发展可能有以下迹象/趋势：

- APT 攻击思路越发与 HW 攻击队模式吻合。
- APT 攻击已经开始重视国内办公软件/系统和安全设备的漏洞利用效果。
- APT 攻击思维从单点钓鱼窃取数据向最大化获取内网控制权限转化。
- APT 的部分攻击者具备将 0day 迅速集成武器化并投入使用能力。
- APT 或将延续 2023 年高密度利用新通用漏洞攻击趋势，漏洞利用涉及产品可能覆盖通用办公软件/系统产品、网络安全产品和重要行业专属的上游供应链产品。

4.3. APT 攻击利用向上游供应链攻击趋势明显

在 2023 年 12 月，东南亚 APT 组织疑似利用某云资产作为跳板针对能源供应链等单位发起网络攻击，利用数据分析模型结合关联分析事件关联链路分析如下：

- 在 2023 年 12 月 21 日，疑似利用某云资产对某办公应用系统供应商资产进行漏洞扫描和信息采集。
- 在 2023 年 12 月 26 日，利用某防火墙漏洞攻击某能源供应商并植入远控木马，在此之前该供应商已经被同源攻击者多次攻击，且进入内网横移和尝试供应链污染。
- 在 2023 年 12 月 27 日，存在与安全厂商 CDN 资产关联痕迹。

地址：北京市东城区朝阳门北大街 19 号 4 层
网址：www.ctct.cn
电话：400-925-9120

➢ 在 2024 年 1 月 3 日，利用某安全网关漏洞攻击某企业，植入同源远控木马。

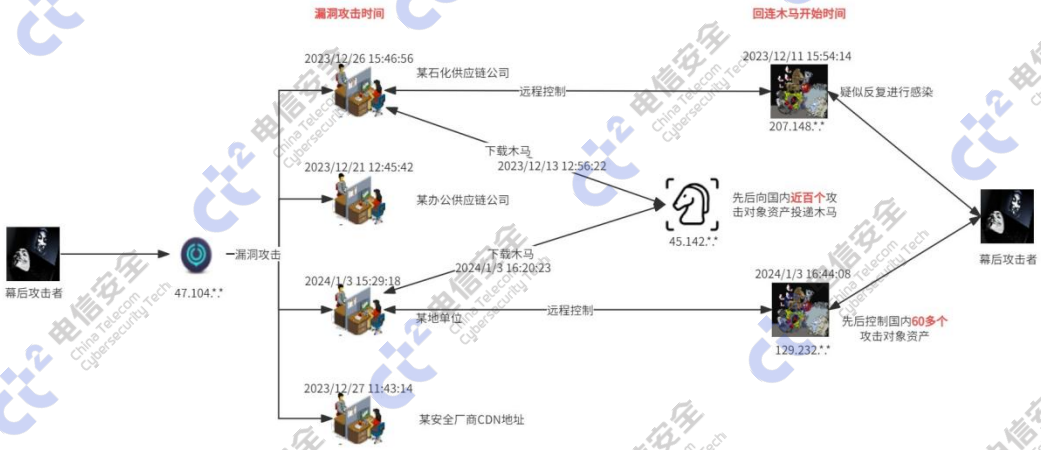


图-能源行业上游供应链攻击复原

该案例并非该组织首次利用上游供应链攻击能源行业，在 2022 年已有类似案例，且在 2023 年有多个类似案例攻击其他行业。说明上游供应链攻击模式的应用对该组织来说已然成熟，后期使用该模式攻击能源、金融、通讯、交通等行业的趋势会更加明显。

4.4.APT 由传统定向攻击延伸非传统攻击

我国深入实施数字经济发展战略，不断完善数字基础设施，加快培育新业态新模式，推进数字产业化和产业数字化取得积极成效。比如物联网建设已然成熟且大面积覆盖，数字政务网已全面推广，智能交通、智能电控和车联网已加速推进建设，而对应的网络安全风险也开始显现。2023 年监测到境外 APT 组织对国内数字政务的数字中心和智能交通、智能电控的供应链上游企业攻击，攻击者一旦在这些企业获取长期网络控制权限，将对国内政务、交通和能源等行业造成极大威胁。

非传统的物联网与车联网看似与 APT 攻击本质目的（窃取数据或制造混乱）没有太大关系，但在某种非常规需求场景下 APT 攻击物联网与车联网可能会有事半功倍的效果。例如，某地区政府在对华情报布局受挫情况下，需要利用 APT 攻击物联网或车联网资产填补定向情报监测需求。

因此，预测 2024 年的 APT 威胁除了在传统行业的数字政务网、智能交通、智能电控基础上向高新科技、通信等行业拓展外，还会向非传统的物联网与车联网延伸。

4.5.APT 与勒索结合的双模式加持攻击

APT&勒索联合加持或许是后续高级黑产团伙的发展趋势，因为大部分批量式攻击获取的勒索对象资产，往往是安全需求不强烈且没有充裕资金做安全建设的中小企业，因此没有更多资金做数据回赎，而大型甚至央/国企业（金融，能源，通信，基建，交通）在安全建设上已有一定的高度，量式攻击突破概率微小，只能与 APT 模式结合加持攻击。2023 年 5

地址：北京市东城区朝阳门北大街 19 号 4 层
网址：www.ctct.cn
电话：400-925-9120

月新出现的高级勒索组织 Rhysida 就是向 APT 攻击模式转型的典型。

据统计，Rhysida 团伙的攻击对象为 40 余个，其中国内攻击对象只有 2 个，相比于其他勒索组织的批量式攻击，Rhysida 团伙的攻击似有“墨鱼现象”，其攻击对象大都具有深度和影响力：例如 2023 年 5 月，Rhysida 攻击智利陆军，7 月攻击了科威特卫生部，8 月攻击了美国医院集团，11 月攻击了大英图书馆、斯洛文尼亚能源部和国内某企业等，都窃取了大量敏感数据并在暗网售卖。

发生时间	事件单位	详细事件描述	数据窃取量	勒索资金
2023 年 5 月	智利陆军	Rhysida 黑客攻击了智利陆军的网站和电子邮件系统，对其数据进行加密。Rhysida还在其泄密网站上泄露了一些数据，包括军事文件以及士兵和军官的个人信息。	——	190万美元
2023 年 7 月	科威特卫生部	Rhysida 攻击了科威特卫生部，对其数据进行加密，还在其泄露网站上泄露了部分数据，包括患者和工作人员的医疗记录以及个人信息。		190万美元
2023 年 8 月	美国医院集团	Rhysida攻击美国医院集团，声称已经窃取了的 SQL 数据库和 1 TB 的文档，包括患者记录、公司文档和 500,000 个社会安全号码。	1.3+ 1 TB	130万美元
2023 年 11月	大英图书馆	Rhysida 攻击全球最大的图书馆之一大英图书馆	612GB	740万美元
2023 年 11月	斯洛文尼亚	公共事业能源基础设施的战略企业，窃取包含能源企业的机密国家数据、方案和计划。		190万美元
2023 年 11月	国内事件单位	Rhysida 攻击国内某单位。		
2024年1月	国内某公司境外机构	Rhysida 攻击国内某企业境外分支机构，并窃取内部数据。		

表-Rhysida 历史攻击事件

联合分析报告和事件线索复盘 Rhysida 组织的攻击画像，其攻击手法和意图都极具 APT 攻击思维，详细攻击画像如下：

- 常用钓鱼邮件方式向攻击对象终端中植入 go 编译的 PortStarter 商业远控木马，获取设备控制权限。为了隐蔽攻击或可视化操作，攻击者有时可能会使用 anydesk 进行远程控制；
- 在控制终端设置 VPN 作为内网穿透隧道；
- ps1 执行系统内置工具获取系统/域信息；
- 利用 ZeroLogon 漏洞进行提权，获取更高域控权限；
- 利用 secretsdump 从系统中进行 NTDS 提取凭据和其他机密信息；
- 利用 ntdsutil 从域控提取并转储用户的哈希值数据库，窃取用户登录凭证；
- 通过 RDP/Psexec.exe/Poershell/Putty 等方式横移登录重要文件服务器、数据库和终端；
- 采集重要数据回传到境外攻击者的仓储站点；
- 利用 wevtutil.exe 清除系统事件日志信息，清除痕迹。

最后在正常程序中注入加密木马执行数据加密，使用 RAS & Chacha20 双重算法加密。

地址：北京市东城区朝阳门北大街 19 号 4 层
网址：www.ctct.cn
电话：400-925-9120

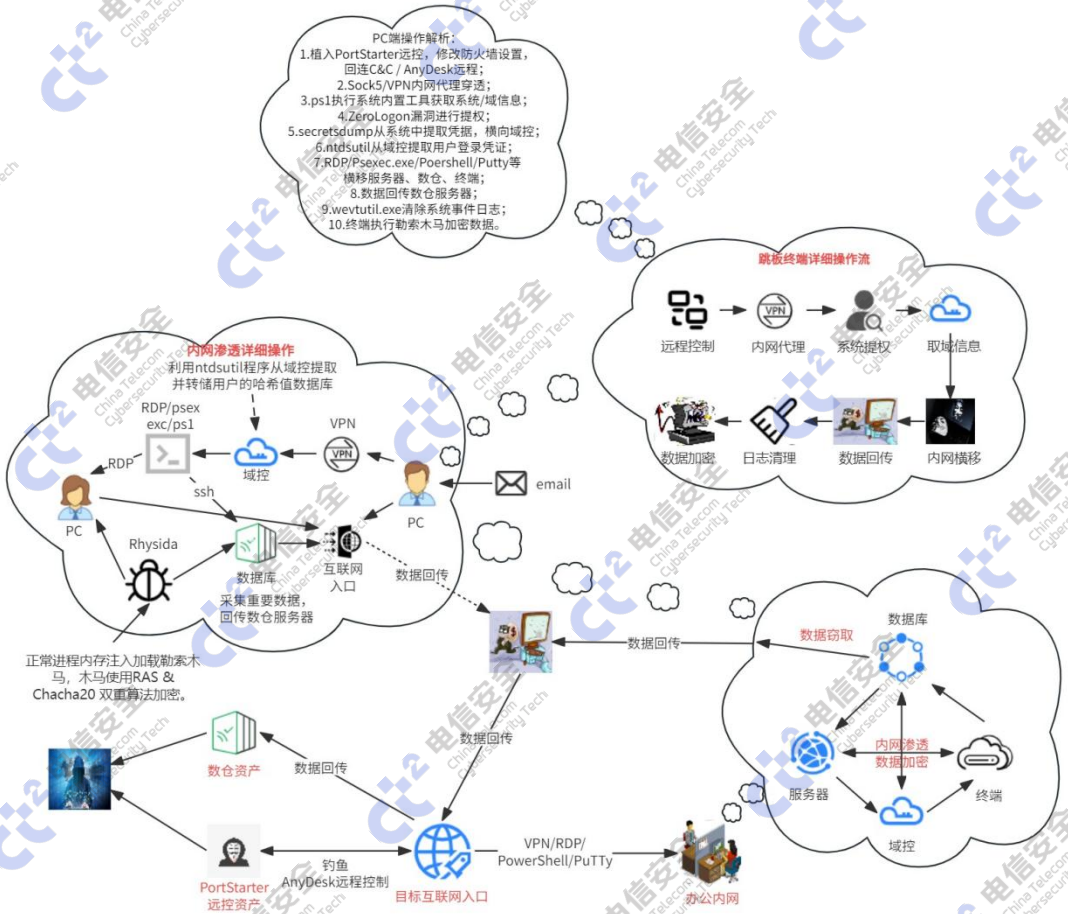


图-Rhysida 攻击事件链路画像

回溯 Rhysida 组织某攻击事件多维信息并利用模型转化威胁风险分析。

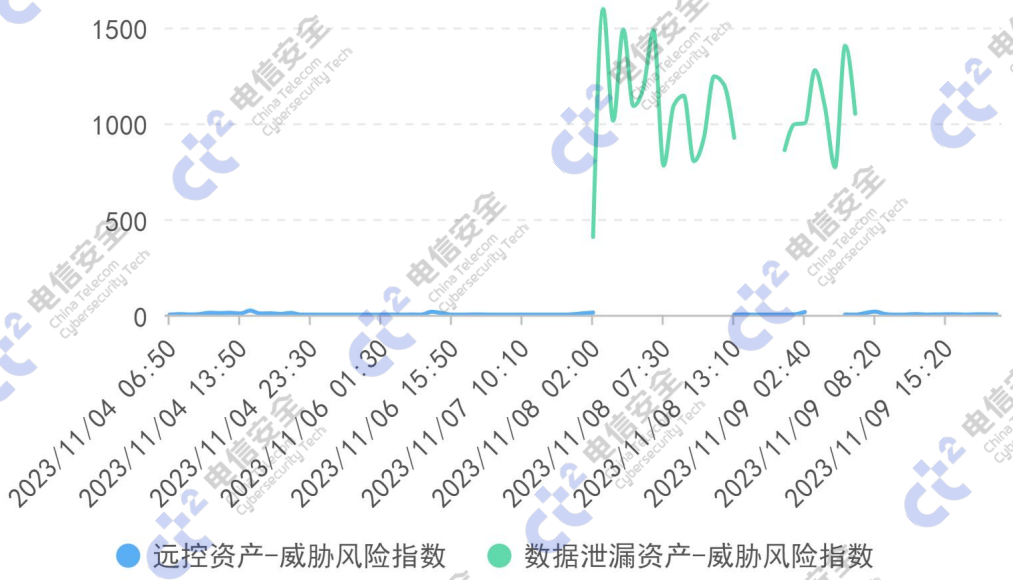


图-事件威胁风险指数分析

攻击者在 11 月 4 日 06:53 获取攻击对象内部终端远程控制权限，攻击对象出现远程回连攻击资产的威胁风险，攻击者开始对攻击对象持续 6 天内网渗透攻击。2023 年 11 月 8 日 01:40，攻击对象出现高烈度的数据回传数仓资产；2023 年 11 月 9 日 06:40，回传数仓威胁风险终止，但远程控制的回连仍然持续；2023 年 11 月 9 日 21:00，远程控制回连中断，风险清除。

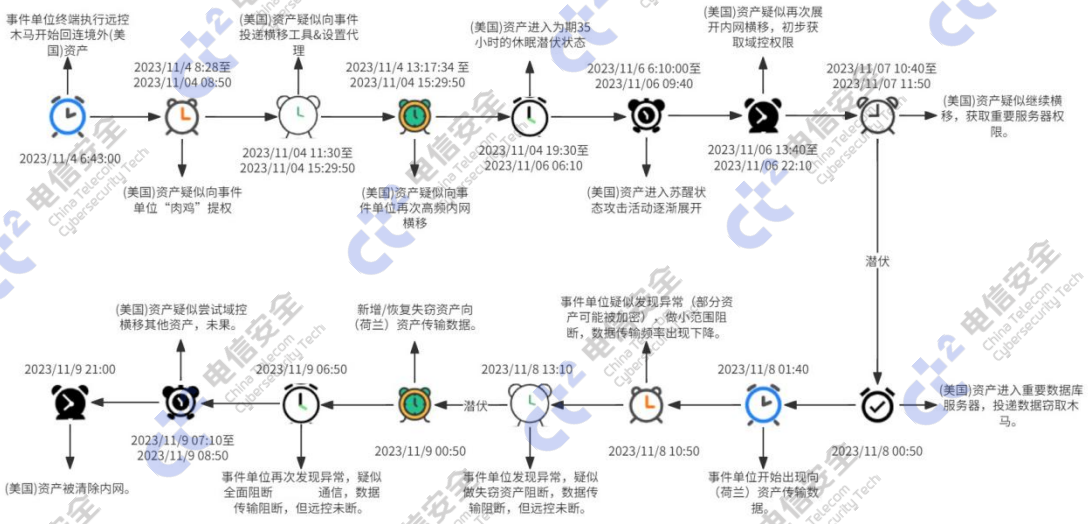


图-事件攻击画像拟真复盘

地址：北京市东城区朝阳门北大街 19 号 4 层
网址：www.ctct.cn
电话：400-925-9120

4.6.数据外泄风险趋势加剧

在 2023 年监测到的各专项攻击中，逆向评估出数据泄露总量约 700+G，然而这只是发现专项攻击可能造成的数据泄露量，而真正具有明显数据泄露威胁的是来自境外勒索团伙的攻击，因为勒索团伙在暗网出售与中国有关的数据量远不止 700+G。

在数字经济将继续朝着信息化、数字化、智能化等方向发展的大背景下，数据是经济发展的重要基石。因此，2024 年仍是数字安全大年，也将是境外对国内勒索或勒索&APT 结合攻击的大年，数据外泄风险趋势将持续加剧，数据防泄漏安全建设任重道远。

专项攻击数据泄露信息分析			
名称	时间段	数据泄露量估算（单位：G）	攻击性质
“尼格风暴”	2022年11月至2023年4月	10+	APT攻击，远程控制
“九霄行动”	2023年1月至2023年7月	52+	APT攻击，窃取数据
“暗云风暴”	2023年8月-	10+	APT攻击，远程控制
“丝绸风暴”	2023年10月至2023年12月	10+	APT攻击，远程控制
“军刀行动”	2023年10月至2024年1月	10+	APT攻击，窃取数据
Mallox勒索专项	2023年11月至2023年12月	30+	勒索攻击，窃取数据
BlackCat勒索专项	2023年12月-	10	勒索攻击，窃取数据
某高级专项		600+	APT攻击，窃取数据

表-专项攻击数据泄露信息分析

5.关于 2024 年安全建设方向的建议

结合国内 2023 年的 APT 攻击威胁态势与 2024 年安全威胁发展预测，国内安全建设或许可以从以下方向入手：

- 前置狩猎、全面感知威胁

新一代的网络安全建设，不能单纯依托点状模式的企业被动威胁识别进行防御，需要主动狩猎安全威胁，常态化追踪攻击组织/团伙活动状态，全面感知其最新武器库、攻击手法、攻击资产、攻击链路、攻击方向、攻击范围、攻击对象、攻击目的等信息补充攻击画像，实现立体式刻画黑客画像。

- 前置评估关基资产假想威胁

在面对未知安全威胁，不能单纯地依靠被动感知，需要主动狩猎未知威胁，捕捉隐藏攻

地址：北京市东城区朝阳门北大街 19 号 4 层
网址：www.ctct.cn
电话：400-925-9120

击的蛛丝马迹，挖掘更深的未知线索。因此，需要从攻击幕后角度思考攻击需求和攻击方向，假想可能会攻击的行业和企业，需要用攻击者思维假想可能存在的攻击路径，落地前置评估核实重要资产假想威胁。

- 前置预警、联防联控

在前置狩猎、前置评估的基础上获取全面感知威胁状态，需要将威胁风险通过联防联控方式落地前置预警，形成一点威胁全面预警的联防联控状态。如今的攻防博弈特别是敌我矛盾的专项攻击，不应该只强调个别企业安全建设的全面化，更需要从全局角度建设群策群力联防联控的“万里长城”。

- 常态化数据安全威胁监测

2024 年仍是数字安全大年，而数据安全是数字经济发展的基础，保护数据安全就是为数字经济发展保驾护航，但不少企业的数据安全建设还处在数据灾备、数据防勒索的阶段，对数据失窃/外泄威胁是后知后觉甚至不知不觉。因此，无论企业还是行业抑或是国家，常态化数据安全威胁监测防止数据失窃，是数据安全建设上新的“战术堡垒”。

- 天下大势，攻就必知，知就必防

2023 年监测到的 APT 事件平均威胁周期 10 天以上。天下大势，攻久必知，知久必防，这可能是目前面对 APT 攻击威胁的写照，但不应该是建设网络安全强国工匠的终点。后期针对 APT 攻击威胁，可以加强前置狩猎、前置评估、全面评估、联防联控、常态化威胁监测的建设。实现天下大势，攻就必知，知就必防的攻守易势，是在建设网络强国道路上，国家对我们每一个网络安全守护者的期望、责任与义务。